Introduction to Modern Algebra

Part IX. Factorization

VII.45. Unique Factorization Domains
| 1 | Lemma 45.9.                                      |
| 2 | Lemma 45.10. The Ascending Chain Condition for a PID |
| 3 | Theorem 45.11.                                   |
| 4 | Lemma 45.12.                                     |
| 5 | Lemma 45.13.                                     |
| 6 | Theorem 45.17.                                   |
| 7 | Corollary 45.18 Fundamental Theorem of Arithmetic. |
| 8 | Lemma 45.23.                                     |
| 9 | Lemma 45.25 Gauss’s Lemma.                       |
| 10| Lemma 45.27.                                     |
| 11| Corollary 45.28.                                 |
| 12| Theorem 45.29.                                   |
| 13| Corollary 45.30.                                 |
Lemma 45.9. Let $R$ be a commutative ring and let $N_1 \subseteq N_2 \subseteq \ldots$ be an ascending chain of ideals $N_i$ in $R$. Then $N = \sup_i N_i$ is an ideal of $R$.

Proof Let $a, b \in N$. Then there are ideals $N_i$ and $N_j$ in the chain with $a \in N_i$ and $b \in N_j$. WLOG, $N_i \subseteq N_j$ and $a, b \in N_j$. 
Lemma 45.9. Let $R$ be a commutative ring and let $N_1 \subseteq N_2 \subseteq \ldots$ be an ascending chain of ideals $N_i$ in $R$. Then $N = \sup_i N_i$ is an ideal of $R$.

Proof Let $a, b \in N$. Then there are ideals $N_i$ and $N_j$ in the chain with $a \in N_i$ and $b \in N_j$. WLOG, $N_i \subseteq N_j$ and $a, b \in N_j$. Every ideal is an additive subgroup, so $a \pm b \in N_j$. By the definition of ideal, $ab \in N_j$. So $a \pm b, ab \in N$. 
Lemma 45.9. Let $R$ be a commutative ring and let $N_1 \subseteq N_2 \subseteq \ldots$ be an ascending chain of ideals $N_i$ in $R$. Then $N = \sup_i N_i$ is an ideal of $R$.

Proof Let $a, b \in N$. Then there are ideals $N_i$ and $N_j$ in the chain with $a \in N_i$ and $b \in N_j$. WLOG, $N_i \subseteq N_j$ and $a, b \in N_j$. Every ideal is an additive subgroup, so $a \pm b \in N_j$. By the definition of ideal, $ab \in N_j$. So $a \pm b, ab \in N$.

Since $0 \in N_i$ for all $i$, it follows that for all $b \in N$, we have $-b \in N$ and $0 \in N$. By Exercise 18.48, $N$ is a subring of $R$. 
Lemma 45.9. Let $R$ be a commutative ring and let $N_1 \subseteq N_2 \subseteq \ldots$ be an ascending chain of ideals $N_i$ in $R$. Then $N = \sup_i N_i$ is an ideal of $R$.

Proof Let $a, b \in N$. Then there are ideals $N_i$ and $N_j$ in the chain with $a \in N_i$ and $b \in N_j$. WLOG, $N_i \subseteq N_j$ and $a, b \in N_j$. Every ideal is an additive subgroup, so $a \pm b \in N_j$. By the definition of ideal, $ab \in N_j$. So $a \pm b, ab \in N$.
Since $0 \in N_i$ for all $i$, it follows that for all $b \in N$, we have $-b \in N$ and $0 \in N$. By Exercise 18.48, $N$ is a subring of $R$. For $a \in N$ and $r \in R$, we have $a \in N_i$ for some $i$ and since $N_i$ is an ideal, then $da = ad \in N_i$. 
**Lemma 45.9.** Let $R$ be a commutative ring and let $N_1 \subseteq N_2 \subseteq \ldots$ be an ascending chain of ideals $N_i$ in $R$. Then $N = \sup_i N_i$ is an ideal of $R$.

**Proof** Let $a, b \in N$. Then there are ideals $N_i$ and $N_j$ in the chain with $a \in N_i$ and $b \in N_j$. WLOG, $N_i \subseteq N_j$ and $a, b \in N_j$. Every ideal is an additive subgroup, so $a \pm b \in N_j$. By the definition of ideal, $ab \in N_j$. So $a \pm b, ab \in N$.

Since $0 \in N_i$ for all $i$, it follows that for all $b \in N$, we have $-b \in N$ and $0 \in N$. By Exercise 18.48, $N$ is a subring of $R$. For $a \in N$ and $r \in R$, we have $a \in N_i$ for some $i$ and since $N_i$ is an ideal, then $da = ad \in N_i$. So $ad \in \cup_i N_i$ and $da \in N$. So $N$ is an ideal of $R$. \qed
Lemma 45.9. Let $R$ be a commutative ring and let $N_1 \subseteq N_2 \subseteq \ldots$ be an ascending chain of ideals $N_i$ in $R$. Then $N = \sup_i N_i$ is an ideal of $R$.

**Proof** Let $a, b \in N$. Then there are ideals $N_i$ and $N_j$ in the chain with $a \in N_i$ and $b \in N_j$. WLOG, $N_i \subseteq N_j$ and $a, b \in N_j$. Every ideal is an additive subgroup, so $a \pm b \in N_j$. By the definition of ideal, $ab \in N_j$. So $a \pm b, ab \in N$.

Since $0 \in N_i$ for all $i$, it follows that for all $b \in N$, we have $-b \in N$ and $0 \in N$. By Exercise 18.48, $N$ is a subring of $R$. For $a \in N$ and $r \in R$, we have $a \in N_i$ for some $i$ and since $N_i$ is an ideal, then $da = ad \in N_i$. So $ad \in \bigcup_i N_i$ and $da \in N$. So $N$ is an ideal of $R$. \qed
Lemma 45.10. The Ascending Chain Condition for a PID. Let $D$ be a PID. If $N_1 \subseteq N_2 \subseteq \ldots$ is an ascending chain of ideals, then there exists a positive integer $r$ such that $N_r = N_s$ for all $s \geq r$. Equivalently, every strictly ascending chain of ideals in a PID is of finite length. Under such conditions it is said that the *ascending chain condition* holds for ideals in a PID.

Proof. By Lemma 45.9, we have that $N = \bigcup_i N_i$ is an ideal of $D$. Since $D$ is a PID then $N$ is a principal ideal and so $N = \langle c \rangle$ for some $c \in D$. 


Lemma 45.10. The Ascending Chain Condition for a PID. Let $D$ be a PID. If $N_1 \subseteq N_2 \subseteq \ldots$ is an ascending chain of ideals, then there exists a positive integer $r$ such that $N_r = N_s$ for all $s \geq r$. Equivalently, every strictly ascending chain of ideals in a PID is of finite length. Under such conditions it is said that the ascending chain condition holds for ideals in a PID.

Proof. By Lemma 45.9, we have that $N = \bigcup_i N_i$ is an ideal of $D$. Since $D$ is a PID then $N$ is a principal ideal and so $N = \langle c \rangle$ for some $c \in D$. Since $N = \bigcup_i N_i$, then $c \in N_r$ for some $r \in \mathbb{N}$. 
Lemma 45.10. The Ascending Chain Condition for a PID. Let $D$ be a PID. If $N_1 \subseteq N_2 \subseteq \ldots$ is an ascending chain of ideals, then there exists a positive integer $r$ such that $N_r = N_s$ for all $s \geq r$. Equivalently, every strictly ascending chain of ideals in a PID is of finite length. Under such conditions it is said that the ascending chain condition holds for ideals in a PID.

Proof. By Lemma 45.9, we have that $N = \bigcup_i N_i$ is an ideal of $D$. Since $D$ is a PID then $N$ is a principal ideal and so $N = \langle c \rangle$ for some $c \in D$. Since $N = \bigcup_i N_i$, then $c \in N_r$ for some $r \in \mathbb{N}$. For $s \geq r$ we have $\langle c \rangle \subseteq N_r \subseteq N_s \subseteq N = \langle c \rangle$. So $N_r = N_s$ for all $s \geq r$. 

Lemma 45.10. The Ascending Chain Condition for a PID. Let $D$ be a PID. If $N_1 \subseteq N_2 \subseteq \ldots$ is an ascending chain of ideals, then there exists a positive integer $r$ such that $N_r = N_s$ for all $s \geq r$. Equivalently, every strictly ascending chain of ideals in a PID is of finite length. Under such conditions it is said that the ascending chain condition holds for ideals in a PID.

Proof. By Lemma 45.9, we have that $N = \bigcup_i N_i$ is an ideal of $D$. Since $D$ is a PID then $N$ is a principal ideal and so $N = \langle c \rangle$ for some $c \in D$. Since $N = \bigcup_i N_i$, then $c \in N_r$ for some $r \in \mathbb{N}$. For $s \geq r$ we have $\langle c \rangle \subseteq N_r \subseteq N_s \subseteq N = \langle c \rangle$. So $N_r = N_s$ for all $s \geq r$. \qed
Lemma. 45.11. Let $D$ be a PID. Every element that is neither 0 nor a unit of $D$ is a product of irreducibles.

Proof. Let $a \in D$ where '$a$' is neither 0 nor a unit. [We first show that '$a$' has at least one irreducible factor.]
Theorem 45.11.

Lemma. 45.11. Let $D$ be a PID. Every element that is neither 0 nor a unit of $D$ is a product of irreducibles.

Proof. Let $a \in D$ where $'a'$ is neither 0 nor a unit. [We first show that $'a'$ has at least one irreducible factor.]

If $'a'$ itself is irreducible then we are done. If $'a'$ is not irreducible, then $a = a_1 b_1$ where neither $a_1$ or $b_1$ is a unit.
Lemma. 45.11. Let $D$ be a PID. Every element that is neither 0 nor a unit of $D$ is a product of irreducibles.

Proof. Let $a \in D$ where $a$ is neither 0 nor a unit. [We first show that $a$ has at least one irreducible factor.]

If $a$ itself is irreducible then we are done. If $a$ is not irreducible, then $a = a_1 b_1$ where neither $a_1$ or $b_1$ is a unit. Now $\langle a \rangle \subset \langle a_1 \rangle$ by Note 1 Part (1) (if $\langle a \rangle = \langle a_1 \rangle$ then by Note 1 Part (2) $a$ and $a_1$ would be associates, contradicting the fact that neither $a_1$ nor $b_1$ is a unit).
Lemma. 45.11. Let \( D \) be a PID. Every element that is neither 0 nor a unit of \( D \) is a product of irreducibles.

Proof. Let \( a \in D \) where \( 'a' \) is neither 0 nor a unit. [We first show that \( 'a' \) has at least one irreducible factor.]

If \( 'a' \) itself is irreducible then we are done. If \( 'a' \) is not irreducible, then \( a = a_1 b_1 \) where neither \( a_1 \) or \( b_1 \) is a unit. Now \( \langle a \rangle \subset \langle a_1 \rangle \) by Note 1 Part (1) (if \( \langle a \rangle = \langle a_1 \rangle \) then by Note 1 Part (2) \( 'a' \) and \( a_1 \) would be associates, contradicting the fact that neither \( a_1 \) nor \( b_1 \) is a unit). If \( a_1 \) is irreducible then \( a_1 \) is an irreducible factor of \( 'a' \). If not, write \( a_1 = a_2 b_2 \) where neither \( a_2 \) nor \( b_2 \) is a unit.
Theorem 45.11.

Lemma. 45.11. Let $D$ be a PID. Every element that is neither 0 nor a unit of $D$ is a product of irreducibles.

Proof. Let $a \in D$ where '$a$' is neither 0 nor a unit. [We first show that '$a$' has at least one irreducible factor.]

If '$a$' itself is irreducible then we are done. If '$a$' is not irreducible, then $a = a_1b_1$ where neither $a_1$ or $b_1$ is a unit. Now $\langle a \rangle \subset \langle a_1 \rangle$ by Note 1 Part (1) (if $\langle a \rangle = \langle a_1 \rangle$ then by Note 1 Part (2) '$a$' and $a_1$ would be associates, contradicting the fact that neither $a_1$ nor $b_1$ is a unit). If $a_1$ is irreducible then $a_1$ is an irreducible factor of '$a$'. If not, write $a_1 = a_2b_2$ where neither $a_2$ nor $b_2$ is a unit. As above, we have $\langle a_1 \rangle \subset \langle a_2 \rangle$. Continue this process to form a strictly ascending chain $\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \ldots$. 
Theorem 45.11.

Lemma. 45.11. Let $D$ be a PID. Every element that is neither 0 nor a unit of $D$ is a product of irreducibles.

Proof. Let $a \in D$ where 'a' is neither 0 nor a unit. [We first show that 'a' has at least one irreducible factor.]
If 'a' itself is irreducible then we are done. If 'a' is not irreducible, then $a = a_1 b_1$ where neither $a_1$ or $b_1$ is a unit. Now $\langle a \rangle \subset \langle a_1 \rangle$ by Note 1 Part (1) (if $\langle a \rangle = \langle a_1 \rangle$ then by Note 1 Part (2) 'a' and $a_1$ would be associates, contradicting the fact that neither $a_1$ nor $b_1$ is a unit). If $a_1$ is irreducible then $a_1$ is an irreducible factor of 'a'. If not, write $a_1 = a_2 b_2$ where neither $a_2$ nor $b_2$ is a unit. As above, we have $\langle a_1 \rangle \subset \langle a_2 \rangle$. Continue this process to form a strictly ascending chain $\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \ldots$.
By Lemma 45.10, this chain terminates with some $\langle a_r \rangle$ and this $a_r$ must be irreducible (or else we would contruct $\langle a_{r+1} \rangle$ with $\langle a_r \rangle \subset \langle a_{r+1} \rangle$).
**Lemma. 45.11.** Let $D$ be a PID. Every element that is neither 0 nor a unit of $D$ is a product of irreducibles.

**Proof.** Let $a \in D$ where $'a'$ is neither 0 nor a unit. [We first show that $'a'$ has at least one irreducible factor.]

If $'a'$ itself is irreducible then we are done. If $'a'$ is not irreducible, then $a = a_1b_1$ where neither $a_1$ or $b_1$ is a unit. Now $\langle a \rangle \subset \langle a_1 \rangle$ by Note 1 Part (1) (if $\langle a \rangle = \langle a_1 \rangle$ then by Note 1 Part (2) $'a'$ and $a_1$ would be associates, contradicting the fact that neither $a_1$ nor $b_1$ is a unit). If $a_1$ is irreducible then $a_1$ is an irreducible factor of $'a'$. If not, write $a_1 = a_2b_2$ where neither $a_2$ nor $b_2$ is a unit. As above, we have $\langle a_1 \rangle \subset \langle a_2 \rangle$. Continue this process to form a strictly ascending chain $\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \ldots$.

By Lemma 45.10, this chain terminates with some $\langle a_r \rangle$ and this $a_r$ must be irreducible (or else we would construct $\langle a_{r+1} \rangle$ with $\langle a_r \rangle \subset \langle a_{r+1} \rangle$). We now have $a = b_1b_2\ldots b_ra_r$ and so $a_r$ is an irreducible factor of $'a'$.
Lemma. 45.11. Let $D$ be a PID. Every element that is neither 0 nor a unit of $D$ is a product of irreducibles.

Proof. Let $a \in D$ where $a$ is neither 0 nor a unit. [We first show that $a$ has at least one irreducible factor.]
If $a$ itself is irreducible then we are done. If $a$ is not irreducible, then $a = a_1 b_1$ where neither $a_1$ or $b_1$ is a unit. Now $\langle a \rangle \subset \langle a_1 \rangle$ by Note 1 Part (1) (if $\langle a \rangle = \langle a_1 \rangle$ then by Note 1 Part (2) $a$ and $a_1$ would be associates, contradicting the fact that neither $a_1$ nor $b_1$ is a unit). If $a_1$ is irreducible then $a_1$ is an irreducible factor of $a$. If not, write $a_1 = a_2 b_2$ where neither $a_2$ nor $b_2$ is a unit. As above, we have $\langle a_1 \rangle \subset \langle a_2 \rangle$. Continue this process to form a strictly ascending chain $\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \ldots$.
By Lemma 45.10, this chain terminates with some $\langle a_r \rangle$ and this $a_r$ must be irreducible (or else we would construct $\langle a_{r+1} \rangle$ with $\langle a_r \rangle \subset \langle a_{r+1} \rangle$). We now have $a = b_1 b_2 \ldots b_r a_r$ and so $a_r$ is an irreducible factor of $a$. 

Lemma. 45.11. Let $D$ be a PID. Every element that is neither 0 nor a unit of $D$ is a product of irreducibles.

Proof. (Continued) Now that we know 'a' has an irreducible factor, we show that it can be written as a product of irreducible factors.

By above, we have that 'a' (neither 0 nor a unit in $D$) is irreducible or of the form $a = p_1c_1$ for $p_1$ an irreducible and $c_1$ not a unit.
Lemma. 45.11. Let $D$ be a PID. Every element that is neither 0 nor a unit of $D$ is a product of irreducibles.

Proof. (Continued) Now that we know $a$ has an irreducible factor, we show that it can be written as a product of irreducible factors. By above, we have that $a$ (neither 0 nor a unit in $D$) is irreducible or of the form $a = p_1 c_1$ for $p_1$ an irreducible and $c_1$ not a unit. If $c_1$ is not a unit (and of course it’s not 0) then by the argument of the first paragraph we have $\langle a \rangle \subset \langle c_1 \rangle$ and if $c_1$ is not irreducible then $c_1 = p_2 c_2$ for irreducible $p_2$ with $c_2$ not a unit.
Lemma. 45.11. Let \( D \) be a PID. Every element that is neither 0 nor a unit of \( D \) is a product of irreducibles.

Proof. (Continued) Now that we know 'a' has an irreducible factor, we show that it can be written as a product of irreducible factors. By above, we have that 'a' (neither 0 nor a unit in \( D \)) is irreducible or of the form \( a = p_1 c_1 \) for \( p_1 \) an irreducible and \( c_1 \) not a unit. If \( c_1 \) is not a unit (and of course it's not 0) then by the argument of the first paragraph we have \( \langle a \rangle \subset \langle c_1 \rangle \) and if \( c_1 \) is not irreducible then \( c_1 = p_2 c_2 \) for irreducible \( p_2 \) with \( c_2 \) not a unit. Continuing we again get a strictly ascending chain of ideals \( \langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \subset \ldots \). By Lemma 45.10, this chain terminates with some \( c_r = q_r \) that is irreducible (as argued in the first paragraph). Then \( a = p_1 p_2 \ldots p_r q_r \) is a product of irreducibles. \( \square \)
Theorem 45.11. (Continued)

**Lemma. 45.11.** Let $D$ be a PID. Every element that is neither 0 nor a unit of $D$ is a product of irreducibles.

**Proof. (Continued)** Now that we know 'a' has an irreducible factor, we show that it can be written as a product of irreducible factors. By above, we have that 'a' (neither 0 nor a unit in $D$) is irreducible or of the form $a = p_1 c_1$ for $p_1$ an irreducible and $c_1$ not a unit. If $c_1$ is not a unit (and of course it’s not 0) then by the argument of the first paragraph we have $\langle a \rangle \subset \langle c_1 \rangle$ and if $c_1$ is not irreducible then $c_1 = p_2 c_2$ for irreducible $p_2$ with $c_2$ not a unit. Continuing we again get a strictly ascending chain of ideals $\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \subset \ldots$.

By Lemma 45.10, this chain terminates with some $c_r = q_r$ that is irreducible (as argued in the first paragraph). Then $a = p_1 p_2 \ldots p_r q_r$ is a product of irreducibles.
Lemma 45.12.

Lemma. 45.12. An ideal $\langle p \rangle$ in a PID is maximal if and only if $p$ is irreducible.

Proof. Let $\langle p \rangle$ be a maximal ideal of $D$, a PID. Suppose $p = ab$ in $D$. Then by Note 1 Part(1) $\langle p \rangle \subseteq \langle a \rangle$. 
Lemma 45.12. An ideal $\langle p \rangle$ in a PID is maximal if and only if $p$ is irreducible.

Proof. Let $\langle p \rangle$ be a maximal ideal of $D$, a PID. Suppose $p = ab$ in $D$. Then by Note 1 Part(1) $\langle p \rangle \subseteq \langle a \rangle$. If $\langle p \rangle = \langle a \rangle$ then by Note 1 Part(2) ’$a$’ and $p$ are associates and $b$ is a unit. If $\langle p \rangle \neq \langle a \rangle$ then since $\langle p \rangle$ is maximal it must be that $\langle a \rangle = D$. 
Lemma 45.12. An ideal $\langle p \rangle$ in a PID is maximal if and only if $p$ is irreducible.

Proof. Let $\langle p \rangle$ be a maximal ideal of $D$, a PID. Suppose $p = ab$ in $D$. Then by Note 1 Part(1) $\langle p \rangle \subseteq \langle a \rangle$. If $\langle p \rangle = \langle a \rangle$ then by Note 1 Part(2) 'a' and $p$ are associates and $b$ is a unit. If $\langle p \rangle \neq \langle a \rangle$ then since $\langle p \rangle$ is maximal it must be that $\langle a \rangle = D$. From the definition of "ideal in D" we have $D = \langle 1 \rangle$, so in this case $\langle a \rangle = \langle 1 \rangle$ and by Note 1 Part(2), 'a' and 1 are associates and hence 'a' is a unit. Thus, if $p = ab$ then either 'a' is a unit or $b$ is a unit; that is, $p$ is irreducible.
Lemma 45.12. An ideal \( \langle p \rangle \) in a PID is maximal if and only if \( p \) is irreducible.

Proof. Let \( \langle p \rangle \) be a maximal ideal of \( D \), a PID. Suppose \( p = ab \) in \( D \). Then by Note 1 Part(1) \( \langle p \rangle \subseteq \langle a \rangle \). If \( \langle p \rangle = \langle a \rangle \) then by Note 1 Part(2) \( 'a' \) and \( p \) are associates and \( b \) is a unit. If \( \langle p \rangle \neq \langle a \rangle \) then since \( \langle p \rangle \) is maximal it must be that \( \langle a \rangle = D \). From the definition of "ideal in \( D \)" we have \( D = \langle 1 \rangle \), so in this case \( \langle a \rangle = \langle 1 \rangle \) and by Note 1 Part(2), \( 'a' \) and \( 1 \) are associates and hence \( 'a' \) is a unit. Thus, if \( p = ab \) then either \( 'a' \) is a unit or \( b \) is a unit; that is, \( p \) is irreducible.
Lemma 45.12. (Continued)

Lemma 45.12. An ideal \( \langle p \rangle \) in a PID is maximal if and only if \( p \) is irreducible.

Proof. (Continued) Conversely, suppose that \( p \) is an irreducible in \( D \). If \( \langle p \rangle \subseteq \langle a \rangle \) then by Note 1 Part(1) we must have \( p = ab \) for some \( b \) in \( D \). If \( 'a' \) is a uit, then \( 'a' \) and 1 are associates and by Note 1 Part(2), we have \( \langle a \rangle = \langle 1 \rangle = D \) and \( \langle a \rangle \) is a maximal ideal. If \( 'a' \) is not a unit, then \( b \) must be a unit (since \( p \) is irreducible) so there exists \( u \in D \) such that \( bu = 1 \).
Lemma 45.12. (Continued)

**Lemma. 45.12.** An ideal $\langle p \rangle$ in a PID is maximal if and only if $p$ is irreducible.

**Proof. (Continued)** Conversely, suppose that $p$ is an irreducible in $D$. If $\langle p \rangle \subseteq \langle a \rangle$ then by Note 1 Part(1) we must have $p = ab$ for some $b$ in $D$. If '$a'$ is a uit, then '$a'$ and 1 are associates and by Note 1 Part(2), we have $\langle a \rangle = \langle 1 \rangle = D$ and $\langle a \rangle$ is a maximal ideal. If '$a'$ is not a unit, then $b$ must be a unit (since $p$ is irreducible) so there exists $u \in D$ such that $bu = 1$. Then $pu = abu = a$ and by Note 1 Part(1) $\langle a \rangle \subseteq \langle p \rangle$ and since $p$ and '$a'$ are associates, by Note 1 Part (2) we have $\langle a \rangle = \langle p \rangle$. 
Lemma 45.12. (Continued)

Lemma. 45.12. An ideal $\langle p \rangle$ in a PID is maximal if and only if $p$ is irreducible.

Proof. (Continued) Conversely, suppose that $p$ is an irreducible in $D$. If $\langle p \rangle \subseteq \langle a \rangle$ then by Note 1 Part(1) we must have $p = ab$ for some $b$ in $D$. If 'a' is a uit, then 'a' and 1 are associates and by Note 1 Part(2), we have $\langle a \rangle = \langle 1 \rangle = D$ and $\langle a \rangle$ is a maximal ideal. If 'a' is not a unit, then $b$ must be a unit (since $p$ is irreducible) so there exists $u \in D$ such that $bu = 1$. Then $pu = abu = a$ and by Note 1 Part(1) $\langle a \rangle \subseteq \langle p \rangle$ and since $p$ and 'a' are associates, by Note 1 Part (2) we have $\langle a \rangle = \langle p \rangle$. We have now shown that if $\langle p \rangle \subseteq \langle a \rangle$ then either $\langle a \rangle = D$ (if 'a' is a unit) or $\langle a \rangle = \langle p \rangle$ (if 'a' is not a unit).
Lemma 45.12. (Continued)

**Lemma. 45.12.** An ideal $\langle p \rangle$ in a PID is maximal if and only if $p$ is irreducible.

**Proof. (Continued)** Conversely, suppose that $p$ is an irreducible in $D$. If $\langle p \rangle \subseteq \langle a \rangle$ then by Note 1 Part(1) we must have $p = ab$ for some $b$ in $D$. If '$a'$ is a unit, then '$a'$ and 1 are associates and by Note 1 Part(2), we have $\langle a \rangle = \langle 1 \rangle = D$ and $\langle a \rangle$ is a maximal ideal. If '$a'$ is not a unit, then $b$ must be a unit (since $p$ is irreducible) so there exists $u \in D$ such that $bu = 1$. Then $pu = abu = a$ and by Note 1 Part(1) $\langle a \rangle \subseteq \langle p \rangle$ and since $p$ and '$a'$ are associates, by Note 1 Part (2) we have $\langle a \rangle = \langle p \rangle$. We have now shown that if $\langle p \rangle \subseteq \langle a \rangle$ then either $\langle a \rangle = D$ (if '$a'$ is a unit) or $\langle a \rangle = \langle p \rangle$ (if '$a'$ is not a unit).
Lemma 45.12. An ideal \( \langle p \rangle \) in a PID is maximal if and only if \( p \) is irreducible.

Proof. (Continued) So there is no proper ideal of \( D \) which properly contains \( \langle p \rangle \) (of course all ideals of \( D \) are principal). That is, \( \langle p \rangle \) is a maximal ideal.
Lemma 45.13. In a PID, if an irreducible $p$ divides $ab$ then either $p \mid a$ or $p \mid b$.

Proof. Let $D$ be a PID and suppose that for an irreducible $p \in D$ we have $p \mid ab$. Then $ab \in \langle p \rangle$ (since $\langle p \rangle$ consists of all multiples of $p$).
Lemma 45.13. In a PID, if an irreducible $p$ divides $ab$ then either $p \mid a$ or $p \mid b$.

Proof. Let $D$ be a PID and suppose that for an irreducible $p \in D$ we have $p \mid ab$. Then $ab \in \langle p \rangle$ (since $\langle p \rangle$ consists of all multiples of $p$). Since $p$ is irreducible, by Lemma 45.12 $\langle p \rangle$ is a maximal ideal in $D$. By Corollary 27.16, every maximal ideal is a prime ideal, so $\langle p \rangle$ is a prime ideal.
**Lemma 45.13.** In a PID, if an irreducible $p$ divies $ab$ then either $p | a$ or $p | b$.

**Proof.** Let $D$ be a PID and suppose that for an irreducible $p \in D$ we have $p | ab$. Then $ab \in \langle p \rangle$ (since $\langle p \rangle$ consists of all multiples of $p$). Since $p$ is irreducible, by Lemma 45.12 $\langle p \rangle$ is a maximal ideal in $D$. By Corollary 27.16, every maximal ideal is a prime ideal, so $\langle p \rangle$ is a prime ideal. Then $ab \in \langle p \rangle$ implies that either $a \in \langle p \rangle$ or $b \in \langle p \rangle$. That is, by Note 1 Part (1), either $p | a$ or $p | b$. \qed
Lemma 45.13. In a PID, if an irreducible $p$ divides $ab$ then either $p \mid a$ or $p \mid b$.

Proof. Let $D$ be a PID and suppose that for an irreducible $p \in D$ we have $p \mid ab$. Then $ab \in \langle p \rangle$ (since $\langle p \rangle$ consists of all multiples of $p$). Since $p$ is irreducible, by Lemma 45.12 $\langle p \rangle$ is a maximal ideal in $D$. By Corollary 27.16, every maximal ideal is a prime ideal, so $\langle p \rangle$ is a prime ideal. Then $ab \in \langle p \rangle$ implies that either $a \in \langle p \rangle$ or $b \in \langle p \rangle$. That is, by Note 1 Part (1), either $p \mid a$ or $p \mid b$. \qed
**Theorem 45.17.** Every PID is a UFD

**Proof.** Theorem 45.11 shows that every PID satisfies the first property of a UFD and gives for $a$ in a PID $D$ where 'a' is neither 0 nor a unit, a factorization $a = p_1 p_2 \cdots p_r$ into irreducibles. Property 2 of a UFD says that such a factorization is unique (in terms of associates).
Theorem 45.17. Every PID is a UFD

Proof. Theorem 45.11 shows that every PID satisfies the first property of a UFD and gives for $a$ in a PID $D$ where $a$ is neither 0 nor a unit, a factorization $a = p_1 p_2 \cdots p_r$ into irreducibles. Property 2 of a UFD says that such a factorization is unique (in terms of associates). Let $a = q_1 q_2 \cdots q_s$ be another factorization of $a$ into irreducibles. Then we have $p_1 | (q_1 q_2 \cdots q_s)$. By Corollary 45.14, $p_1 | q_j$ for some $j$. Reorder the $q$’s such that $q_j$ becomes $q_1$. 
Theorem 45.17. Every PID is a UFD

Proof. Theorem 45.11 shows that every PID satisfies the first property of a UFD and gives for \( a \) in a PID \( D \) where \( 'a' \) is neither 0 nor a unit, a factorization \( a = p_1 p_2 \cdots p_r \) into irreducibles. Property 2 of a UFD says that such a factorization is unique (in terms of associates). Let \( a = q_1 q_2 \cdots q_s \) be another factorization of \( 'a' \) into irreducibles. Then we have \( p_1 \mid (q_1 q_2 \cdots q_s) \). By Corollary 45.14, \( p_1 \mid q_j \) for some \( j \). Reorder the \( q \)'s such that \( q_j \) becomes \( q_1 \). Then \( q_1 = p_1 u_1 \) where \( u_1 \) is a unit. Then \( p_1 \) and \( q_1 \) are associates. Then \( p_1 p_2 \cdots p_r = (p_1 u_1) q_1 q_2 \cdots q_s \). By cancellation in integral domain \( D \) (Theorem 19.5) \( p_2 p_3 \cdots p_r = u_1 q_1 q_2 \cdots q_s \).
Theorem. 45.17. Every PID is a UFD

Proof. Theorem 45.11 shows that every PID satisfies the first property of a UFD and gives for \( a \) in a PID \( D \) where \( \not\exists a \) is neither 0 nor a unit, a factorization \( a = p_1 p_2 \cdots p_r \) into irreducibles. Property 2 of a UFD says that such a factorization is unique (in terms of associates). Let \( a = q_1 q_2 \cdots q_s \) be another factorization of \( \not\exists a \) into irreducibles. Then we have \( p_1 \mid (q_1 q_2 \cdots q_s) \). By Corollary 45.14, \( p_1 \mid q_j \) for some \( j \). Reorder the \( q \)'s such that \( q_j \) becomes \( q_1 \). Then \( q_1 = p_1 u_1 \) where \( u_1 \) is a unit. Then \( p_1 \) and \( q_1 \) are associates. Then
\[
p_1 p_2 \cdots p_r = (p_1 u_1) q_1 q_2 \cdots q_s. \]
By cancellation in integral domain \( D \) (Theorem 19.5)
\[
p_2 p_3 \cdots p_r = u_1 q_1 q_2 \cdots q_s.\]
Theorem 45.17. Every PID is a UFD

Proof. (Continued) Repeating the process we have
\[ 1 = u_1 u_2 \cdots u_r q_{r+1} \cdots q_s \text{ (WLOG } s \geq r). \]
But if \( s > R \) and we have some \( q \) still present on the right-hand side, say \( q_{r+1} \), then the other elements of the right-hand side are an inverse of the \( q \), for example
\[ (q_{r+1})^{-1} = u_1 u_2 \cdots u_r q_{r+2} q_{r+3} \cdots q_s. \]
But this contradicts the fact that the \( q \)'s are irreducible and so (by definition) not units. So there are no \( q \)’s remaining on the right-hand side and \( r = s \). So \( p_i = u_i q_i \) for \( i = 1, 2, \ldots, r \) and such \( p_i \) is an associate of \( q_i \). This is Property 2 in the definition of a UFD and so \( D \) is a UFD.
Theorem 45.17. (Continued)

Theorem. 45.17. Every PID is a UFD

Proof. (Continued) Repeating the process we have

\[ 1 = u_1 u_2 \cdots u_r q_{r+1} \cdots q_s \] (WLOG \( s \geq r \)). But if \( s > R \) and we have some \( q \) still present on the right-hand side, say \( q_{r+1} \), then the other elements of the right-hand side are an inverse of the \( q \), for example

\[ (q_{r+1})^{-1} = u_1 u_2 \cdots u_r q_{r+2} q_{r+3} \cdots q_s. \]

But this contradicts the fact that the \( q \)'s are irreducible and so (by definition) not units. So there are no \( q \)'s remaining on the right-hand side and \( r = s \). So \( p_i = u_i q_i \) for \( i = 1, 2, \ldots, r \) and such \( p_i \) is an associate of \( q_i \). This is Property 2 in the definition of a UFD and so \( D \) is a UFD.

\[ \square \]
Corollary 45.18 Fundamental Theorem of Arithmetic. The integral domain $\mathbb{Z}$ is a UFD.

**Proof.** We know that $\mathbb{Z}$ is a PID (see the note after Definition 45.7). So by Theorem 45.17, $\mathbb{Z}$ is a UFD.
Lemma 45.23. If $D$ is a UFD then for every nonconstant $f(x) \in D[x]$ we have $f(x) = cg(x)$ where $c \in D$, $g(x) \in D[x]$ and $g(x)$ is a primitive. The element $c$ is unique up to a unit factor in $D$ and is the content of $f(x)$. Also $g(x)$ is unique up to a unit factor in $D$.

Proof. Let $f(x) \in D[x]$ be given where $f(x)$ is a nonconstant polynomial with coefficients $a_0, a_1, ..., a_n$. Let $c$ be a gcd of the $a_i$. Then for each $i$, we have $a_i = cg_i$ for some $g_i \in D$. 
Lemma 45.23. If $D$ is a UFD then for every nonconstant $f(x) \in D[x]$ we have $f(x) = cg(x)$ where $c \in D$, $g(x) \in D[x]$ and $g(x)$ is a primitive. The element $c$ is unique up to a unit factor in $D$ and is the content of $f(x)$. Also $g(x)$ is unique up to a unit factor in $D$.

Proof. Let $f(x) \in D[x]$ be given where $f(x)$ is a nonconstant polynomial with coefficients $a_0, a_1, \ldots, a_n$. Let $c$ be a gcd of the $a_i$. Then for each $i$, we have $a_i = cg_i$ for some $g_i \in D$. We have $f(x) = cg(x)$. Now there is no irreducible dividing all of the $g_i$ (if so, say the irreducible in $b$, then $cb$ divides all $a_i$, but $cb \nmid c$ so in this case $c$ is not a gcd of the $a_i$). So a gcd of the $g_i$ must be a unit and have an associate of 1.
Lemma 45.23. If $D$ is a UFD then for every nonconstant $f(x) \in D[x]$ we have $f(x) = cg(x)$ where $c \in D$, $g(x) \in D[x]$ and $g(x)$ is a primitive. The element $c$ is unique up to a unit factor in $D$ and is the content of $f(x)$. Also $g(x)$ is unique up to a unit factor in $D$.

Proof. Let $f(x) \in D[x]$ be given where $f(x)$ is a nonconstant polynomial with coefficients $a_0, a_1, ..., a_n$. Let $c$ be a gcd of the $a_i$. Then for each $i$, we have $a_i = cg_i$ for some $g_i \in D$. We have $f(x) = cg(x)$. Now there is no irreducible dividing all of the $g_i$ (if so, say the irreducible in $b$, then $cb$ divides all $a_i$, but $cb \nmid c$ so in this case $c$ is not a gcd of the $a_i$). So a gcd of the $g_i$ must be a unit and have an associate of 1. So 1 is a gcd of the $g_i$ and $g(x)$ is a primitive polynomial.
Lemma 45.23. If $D$ is a UFD then for every nonconstant $f(x) \in D[x]$ we have $f(x) = cg(x)$ where $c \in D$, $g(x) \in D[x]$ and $g(x)$ is a primitive. The element $c$ is unique up to a unit factor in $D$ and is the content of $f(x)$. Also $g(x)$ is unique up to a unit factor in $D$.

Proof. Let $f(x) \in D[x]$ be given where $f(x)$ is a nonconstant polynomial with coefficients $a_0, a_1, \ldots, a_n$. Let $c$ be a gcd of the $a_i$. Then for each $i$, we have $a_i = cg_i$ for some $g_i \in D$. We have $f(x) = cg(x)$. Now there is no irreducible dividing all of the $g_i$ (if so, say the irreducible in $b$, then $cb$ divides all $a_i$, but $cb \nmid c$ so in this case $c$ is not a gcd of the $a_i$). So a gcd of the $g_i$ must be a unit and have an associate of 1. So 1 is a gcd of the $g_i$ and $g(x)$ is a primitive polynomial.
Lemma 45.23. If $D$ is a UFD then for every nonconstant $f(x) \in D[x]$ we have $f(x) = cg(x)$ where $c \in D$, $g(x) \in D[x]$ and $g(x)$ is a primitive. The element $c$ is unique up to a unit factor in $D$ and is the content of $f(x)$. Also $g(x)$ is unique up to a unit factor in $D$.

Proof. (Continued) For uniqueness, if $f(x) = dh(x)$ also for some $h \in D$ and $h(x) \in D[x]$ with $h(x)$ primitive, then each irreducible factor of $c$ must divide $d$ and each irreducible factor of $d$ must divide $c$ (or else, as in the first paragraph, 1 is not a gcd of the respective coefficients of $g$ or $h$ and hence $g$ or $h$ is not primitive).

By setting $cg(x) = dh(x)$ (since both equal $f(x)$) and cancelling irreducible factors of $c$ into $d$ (Theorem 19.5), we arrive at $ug(x) = vh(x)$ for a unit $u \in D$. But then $v$ must be a unit of $D$ or we would be able to cancel irreducible factors of $v$ into $u$. 
Lemma 45.23. (Continued)

Lemma. 45.23. If $D$ is a UFD then for every nonconstant $f(x) \in D[x]$ we have $f(x) = cg(x)$ where $c \in D$, $g(x) \in D[x]$ and $g(x)$ is a primitive. The element $c$ is unique up to a unit factor in $D$ and is the content of $f(x)$. Also $g(x)$ is unique up to a unit factor in $D$.

Proof. (Continued) For uniqueness, if $f(x) = dh(x)$ also for some $h \in D$ and $h(x) \in D[x]$ with $h(x)$ primitive, then each irreducible factor of $c$ must divide $d$ and each irreducible factor of $d$ must divide $c$ (or else, as in the first paragraph, 1 is not a gcd of the respective coefficients of $g$ or $h$ and hence $g$ or $h$ is not primitive).

By setting $cg(x) = dh(x)$ (since both equal $f(x)$) and cancelling irreducible factors of $c$ into $d$ (Theorem 19.5), we arrive at $ug(x) = vh(x)$ for a unit $u \in D$. But then $v$ must be a unit of $D$ or we would be able to cancel irreducible factors of $v$ into $u$. 
Lemma 45.23. (Continued)

**Lemma. 45.23.** If $D$ is a UFD then for every nonconstant $f(x) \in D[x]$ we have $f(x) = cg(x)$ where $c \in D$, $g(x) \in D[x]$ and $g(x)$ is a primitive. The element $c$ is unique up to a unit factor in $D$ and is the content of $f(x)$. Also $g(x)$ is unique up to a unit factor in $D$.

**Proof. (Continued)** So $u$ and $v$ are both units and $c$ is unique up to a unit factor (here, $d = v^{-1}uc$). Since $f(x) = cg(x)$, then the primitive polynomial $g(x)$ is also unique up to a unit factor.
Lemma 45.25 Gauss’s Lemma. If \( D \) is a UFD, then a product of two primitive polynomials in \( D[x] \) is again primitive.

Proof. Let \( f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \) and \( g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m \) be primitives in \( D[x] \) and let \( h(x) = f(x)g(x) \). Let \( p \) be an irreducible in \( D \). Then \( p \) does not divide all \( a_i \) and \( p \) does not divide \( b_j \) (or else a multiple of \( p \) is a gcd of the \( a_i \) and of the \( b_j \) and 1 is not a gcd since all gcd’s are associates). [since \( f(x) \) and \( g(x) \) are primitive.]
Lemma 45.25 Gauss’s Lemma. If $D$ is a UFD, then a product of two primitive polynomials in $D[x]$ is again primitive.

Proof. Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ and $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$ be primitives in $D[x]$ and let $h(x) = f(x)g(x)$. Let $p$ be an irreducible in $D$. Then $p$ does not divide all $a_i$ and $p$ does not divide $b_j$ (or else a multiple of $p$ is a gcd of the $a_i$ and of the $b_j$ and 1 is not a gcd since all gcd’s are associates). [since $f(x)$ and $g(x)$ are primitive.]

Let $a_r$ be the first coefficient (i.e., $r$ is the smallest value) of $f(x)$ not divisible by $p$; that is, $p \mid a_i$ for $0 \leq i < r$ but $p \nmid a_r$. Similarly, let $p \mid b_j$ for $0 \leq i < s$ but $p \nmid b_s$. 
Lemma. 45.25 Gauss’s Lemma. If $D$ is a UFD, then a product of two primitive polynomials in $D[x]$ is again primitive.

Proof. Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ and $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$ be primitives in $D[x]$ and let $h(x) = f(x)g(x)$. Let $p$ be an irreducible in $D$. Then $p$ does not divide all $a_i$ and $p$ does not divide $b_j$ (or else a multiple of $p$ is a gcd of the $a_i$ and of the $b_j$ and 1 is not a gcd since all gcd’s are associates). [since $f(x)$ and $g(x)$ are primitive.]

Let $a_r$ be the first coefficient (i.e., $r$ is the smallest value) of $f(x)$ not divisible by $p$; that is, $p \mid a_i$ for $0 \leq i < r$ but $p \nmid a_r$. Similarly, let $p \mid b_j$ for $0 \leq i < s$ but $p \nmid b_s$. 
Lemma. 45.25 Gauss’s Lemma. If $D$ is a UFD, then a product of two primitive polynomials in $D[x]$ is again primitive.

Proof. (Continued) The coefficient of $x^{r+s}$ in $h(x) = f(x)g(x)$ is (we are in a commutative ring):

$$c_{r+s} = (a_0 b_{r+s} + a_1 b_{r+s-1} + \ldots + a_{r-1} b_{s+1}) + a_r b_s$$
$$+ (a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \ldots + a_{r+s} b_0)$$

(1)

Now $p \mid a_i$ for $0 \leq i < r$ implies that $p \mid (a_0 b_{r+s} + a_1 b_{r+s-1} + \ldots + a_{r-1} b_{s+1})$ and $p \mid b_j$ for $0 \leq j < s$ implies that $p \mid (a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \ldots + a_{r+s} b_0)$. 
Lemma 45.25 Gauss’s Lemma. If \( D \) is a UFD, then a product of two primitive polynomials in \( D[x] \) is again primitive.

Proof. (Continued) The coefficient of \( x^{r+s} \) in \( h(x) = f(x)g(x) \) is (we are in a commutative ring):

\[
c_{r+s} = (a_0 b_{r+s} + a_1 b_{r+s-1} + \ldots + a_{r-1} b_{s+1}) + a_r b_s \\
+ (a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \ldots + a_{r+s} b_0)
\]  

(1)

Now \( p \mid a_i \) for \( 0 \leq i < r \) implies that \( p \mid (a_0 b_{r+s} + a_1 b_{r+s-1} + \ldots + a_{r-1} b_{s+1}) \) and \( p \mid b_j \) for \( 0 \leq j < s \) implies that \( p \mid (a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \ldots + a_{r+s} b_0) \).
Lemma. 45.25 Gauss’s Lemma. If $D$ is a UFD, then a product of two primitive polynomials in $D[x]$ is again primitive.

Proof. (Continued) But $p$ does not divide $a_r$ or $b_s$, so $p$ does not divide $a_r b_s$ and consequently $p$ does not divide $c_{r+s}$. So we have that any irreducible $p \in D$ does not divide some coefficient of $f(x)g(x)$. So the gcd of the coefficients of $f(x)g(x)$ is 1 and $f(x)g(x)$ is primitive. □
Lemma 45.27. Let $D$ be a UFD and let $F$ be a field of quotients of $D$. Let $f(x) \in D[x]$ where $(\text{degree } f(x)) > 0$. If $f(x)$ is an irreducible in $D[x]$, then $f(x)$ is also an irreducible in $F[x]$. Also, if $f(x)$ is primitive in $D[x]$ and irreducible in $F[x]$, then $f(x)$ is irreducible in $D[x]$.

Proof. We prove the contrapositive of the first claim. Suppose that a nonconstant $f(x) \in D[x]$ factors into polynomials of lower degree in $F[x]$; that is $f(x) = r(x)s(x)$ for $r(x), s(x) \in F[x]$. Then since $F$ is a field of quotients of $D$, each coefficient in $r(x)$ and $s(x)$ is of the form $a/b$ for some $a, b \in D, b \neq 0$. 
Lemma 45.27. Let $D$ be a UFD and let $F$ be a field of quotients of $D$. Let $f(x) \in D[x]$ where ($\text{degree } f(x)$) $> 0$. If $f(x)$ is an irreducible in $D[x]$, then $f(x)$ is also an irreducible in $F[x]$. Also, if $f(x)$ is primitive in $D[x]$ and irreducible in $F[x]$, then $f(x)$ is irreducible in $D[x]$.

Proof. We prove the contrapositive of the first claim. Suppose that a nonconstant $f(x) \in D[x]$ factors into polynomials of lower degree in $F[x]$; that is $f(x) = r(x)s(x)$ for $r(x), s(x) \in F[x]$. Then since $F$ is a field of quotients of $D$, each coefficient in $r(x)$ and $s(x)$ is of the form $a/b$ for some $a, b \in D$, $b \neq 0$. By "clearing the denominators" (i.e. multiplying through by a common multiple of the denominator) we can get $df(x) = r_1(x)s_1(x)$ for $d \in D$ and $r_1(x), s_1(x) \in D[x]$ where the degrees of $r_1(x)$ and $s_1(x)$ equal the degrees of $r(x)$ and $s(x)$, respectively.
Lemma 45.27. Let $D$ be a UFD and let $F$ be a field of quotients of $D$. Let $f(x) \in D[x]$ where $(\text{degree } f(x)) > 0$. If $f(x)$ is an irreducible in $D[x]$, then $f(x)$ is also an irreducible in $F[x]$. Also, if $f(x)$ is primitive in $D[x]$ and irreducible in $F[x]$, then $f(x)$ is irreducible in $D[x]$.

Proof. We prove the contrapositive of the first claim. Suppose that a nonconstant $f(x) \in D[x]$ factors into polynomials of lower degree in $F[x]$; that is $f(x) = r(x)s(x)$ for $r(x), s(x) \in F[x]$. Then since $F$ is a field of quotients of $D$, each coefficient in $r(x)$ and $s(x)$ is of the form $a/b$ for some $a, b \in D, b \neq 0$. By ”clearing the denominators” (i.e. multiplying through by a common multiple of the denominator) we can get $df(x) = r_1(x)s_1(x)$ for $d \in D$ and $r_1(x), s_1(x) \in D[x]$ where the degrees of $r_1(x)$ and $s_1(x)$ equal the degrees of $r(x)$ and $s(x)$, respectively.
Lemma 45.27. (Continued)

**Lemma. 45.27.** Let $D$ be a UFD and let $F$ be a field of quotients of $D$. Let $f(x) \in D[x]$ where $(\text{degree } f(x)) > 0$. If $f(x)$ is an irreducible in $D[x]$, then $f(x)$ is also an irreducible in $F[x]$. Also, if $f(x)$ is primitive in $D[x]$ and irreducible in $F[x]$, then $f(x)$ is irreducible in $D[x]$.

**Proof. (Continued)** By Lemma 45.23 $f(x) = cg(x)$, $r_1(x) = c_1r_2(x)$, and $s_1(x) = c_2s_2(x)$ for primitive polynomials $g(x)$, $r_2(x)$ and $s_2(x)$ in $D[x]$ and $c, c_1, c_2 \in D$. Then $dcg(x) = c_1r_2(x)c_2s_2(x) = c_1c_2r_2(x)s_2(x)$ and by Lemma 45.25 the product $r_2(x)s_2(x)$ is primitive. By the uniqueness part of Lemma 45.23, $c_1c_2 = dcu$ for some unit $u$ in $D$. But then $d cg(x) = dcur_2(x)s_2(x)$ and so $f(x) = cg(x) = cur_2(x)s_2(x)$ where $cu \in D$ and $r_2(x), s_2(x) \in D[x]$.

So $f(x)$ factors nontrivially into polynomials of the same degree in $D[x]$ as the degree of the polynomial factors of $f(x)$ in $F[x]$.

A nonconstant $f(x) \in D[x]$ that is primitive in $D[x]$ and irreducible in $F[x]$ is also irreducible in $D[x]$ since $D[x] \subseteq F[x]$. 

\[\square\]
Lemma 45.27. (Continued)

**Lemma. 45.27.** Let $D$ be a UFD and let $F$ be a field of quotients of $D$. Let $f(x) \in D[x]$ where $(\text{degree } f(x)) > 0$. If $f(x)$ is an irreducible in $D[x]$, then $f(x)$ is also an irreducible in $F[x]$. Also, if $f(x)$ is primitive in $D[x]$ and irreducible in $F[x]$, then $f(x)$ is irreducible in $D[x]$.

**Proof. (Continued)** By Lemma 45.23 $f(x) = cg(x)$, $r_1(x) = c_1 r_2(x)$, and $s_1(x) = c_2 s_2(x)$ for primitive polynomials $g(x), r_2(x)$ and $s_2(x)$ in $D[x]$ and $c, c_1, c_2 \in D$. Then $d cg(x) = c_1 r_2(x) c_2 s_2(x) = c_1 c_2 r_2(x) s_2(x)$ and by Lemma 45.25 the product $r_2(x) s_2(x)$ is primitive. By the uniqueness part of Lemma 45.23, $c_1 c_2 = d cu$ for some unit $u$ in $D$. But then $d cg(x) = d cur_2(x) s_2(x)$ and so $f(x) = cg(x) = cur_2(x) s_2(x)$ where $cu \in D$ and $r_2(x), s_2(x) \in D[x]$. So $f(x)$ factors nontrivially into polynomials of the same degree in $D[x]$ as the degree of the polynomial factors of $f(x)$ in $F[x]$. A nonconstant $f(x) \in D[x]$ that is primitive in $D[x]$ and irreducible in $F[x]$ is also irreducible in $D[x]$ since $D[x] \subseteq F[x]$. □
Corollary 45.28. If $D$ is a UFD and $F$ is a field of quotients of $D$, then a nonconstant $f(x) \in D[x]$ factors into a product of two polynomials of lower degrees $r$ and $s$ in $F[x]$ if and only if it has a factorization into polynomials of the same degrees $r$ and $s$ in $D[x]$.

Proof. In the proof of Lemma 45.27, if $f(x)$ factors in $F[x]$ into $f(x) = r(x)s(x)$ where $r(x)$ and $s(x)$ are of degrees smaller than the degree of $f(x)$, then $f(x) = cur_2(x)s_2(x)$ in $D[x]$ where the degrees of $r(x)$ and $r_2(x)$ are the same and the degrees of $s(x)$ and $s_2(x)$ are the same. The converse holds since $D[x] \subseteq F[x]$. 

[Proof]
Corollary 45.28. 

**Corollary.** 45.28. If $D$ is a UFD and $F$ is a field of quotients of $D$, then a nonconstant $f(x) \in D[x]$ factors into a product of two polynomials of lower degrees $r$ and $s$ in $F[x]$ if and only if it has a factorization into polynomials of the same degrees $r$ and $s$ in $D[x]$.

**Proof.** In the proof of Lemma 45.27, if $f(x)$ factors in $F[x]$ into 
$f(x) = r(x)s(x)$ where $r(x)$ and $s(x)$ are of degrees smaller than the degree of $f(x)$, then $f(x) = cur_2(x)s_2(x)$ in $D[x]$ where the degrees of $r(x)$ and $r_2(x)$ are the same and the degrees of $s(x)$ and $s_2(x)$ are the same. The converse holds since $D[x] \subseteq F[x]$. □
Theorem 45.29.

**Theorem. 45.29.** If $D$ is a UFD, then $D[x]$ is a UFD.

**Proof.** Let $f(x) \in D[x]$ where $f(x)$ is neither 0 nor a unit. If $f(x)$ is of degree 0, we are done since $D$ is a UFD.
Theorem 45.29. If $D$ is a UFD, then $D[x]$ is a UFD.

**Proof.** Let $f(x) \in D[x]$ where $f(x)$ is neither 0 nor a unit. If $f(x)$ is of degree 0, we are done since $D$ is a UFD. Suppose $(\text{degree } f(x)) > 0$. Let $f(x) = g_1(x)g_2(x) \cdots g_r(x)$ be a factorization of $f(x)$ in $D[x]$ having the greatest number $r$ of factors of positive degree (so no $g_i(x)$ is a constant polynomial). There is such a greatest number of such factors since $r$ cannot exceed the degree of $f(x)$. 


Theorem 45.29.

Theorem 45.29. If $D$ is a UFD, then $D[x]$ is a UFD.

Proof. Let $f(x) \in D[x]$ where $f(x)$ is neither 0 nor a unit. If $f(x)$ is of degree 0, we are done since $D$ is a UFD. Suppose $(\text{degree } f(x)) > 0$. Let $f(x) = g_1(x)g_2(x) \cdots g_r(x)$ be a factorization of $f(x)$ in $D[x]$ having the greatest number $r$ of factors of positive degree (so no $g_i(x)$ is a constant polynomial). There is such a greatest number of such factors since $r$ cannot exceed the degree of $f(x)$. 
Theorem 45.29. (Continued)

Theorem. 45.29. If $D$ is a UFD, then $D[x]$ is a UFD.

Proof. (Continued) Now factor each $g_i(x)$ in the form $g_i(x) = c_i h(x)$ where $c_i$ is the content of $g_i(x)$ (by Lemma 45.23, $c$ is a gcd of the coefficients of $g_i(x)$) and $h_i(x)$ is a primitive polynomial. Also, each $h_i(x)$ must be irreducible; if an $h_i(x)$ could be factored then the corresponding factorization of $g_i(x)$ (described in the proof of Lemma 45.27) would give a factorization of $f(x)$ with more than $r$ factors, contradicting the choice of $r$. 


Theorem 45.29. (Continued)

**Theorem.** 45.29. If $D$ is a UFD, then $D[x]$ is a UFD.

**Proof.** (Continued) Now factor each $g_i(x)$ in the form $g_i(x) = c_i h_i(x)$ where $c_i$ is the content of $g_i(x)$ (by Lemma 45.23, $c$ is a gcd of the coefficients of $g_i(x)$) and $h_i(x)$ is a primitive polynomial. Also, each $h_i(x)$ must be irreducible; if an $h_i(x)$ could be factored then the corresponding factorization of $g_i(x)$ (described in the proof of Lemma 45.27) would give a factorization of $f(x)$ with more than $r$ factors, contradicting the choice of $r$. Thus we now have $f(x) = c_1 h_1(x) c_2 h_2(x) \cdots c_r h_r(x)$ where the $h_i(x)$ are irreducible in $D[x]$. If we now factor the $c_i$ into irreducibles in $D$ (since $D$ is a UFD), we obtain a factorization of $f(x)$ into a product of irreducibles in $D[x]$. 


Theorem 45.29. (Continued)

**Theorem 45.29.** If $D$ is a UFD, then $D[x]$ is a UFD.

**Proof. (Continued)** Now factor each $g_i(x)$ in the form $g_i(x) = c_i h(x)$ where $c_i$ is the content of $g_i(x)$ (by Lemma 45.23, $c$ is a gcd of the coefficients of $g_i(x)$) and $h_i(x)$ is a primitive polynomial. Also, each $h_i(x)$ must be irreducible; if an $h_i(x)$ could be factored then the corresponding factorization of $g_i(x)$ (described in the proof of Lemma 45.27) would give a factorization of $f(x)$ with more than $r$ factors, contradicting the choice of $r$. Thus we now have $f(x) = c_1 h_1(x)c_2 h_2(x) \cdots c_r h_r(x)$ where the $h_i(x)$ are irreducible in $D[x]$. If we now factor the $c_i$ into irreducibles in $D$ (since $D$ is a UFD), we obtain a factorization of $f(x)$ into a product of irreducibles in $D[x]$. 
Theorem 45.29. (Continued)

**Theorem. 45.29.** If $D$ is a UFD, then $D[x]$ is a UFD.

**Proof. (Continued)** The factorization of $f(x) \in D[x]$ where $f(x)$ has degree 0 is unique since $D$ is a UFD. If $f(x)$ has degree greater than 0, then any factorization of $f(x)$ into irreducibles in $D[x]$ corresponds to a factorization in $F[x]$ into units (the factors in $D$; the constant factors) and, by Lemma 45.27, irreducible polynomials in $F[x]$. By Theorem 23.20, these irreducible polynomials are unique, except for possible constant factors in $F$. But as an irreducible in $D[x]$, each polynomial of degree $> 0$ appearing in the factorization of $f(x)$ in $D[x]$ is primitive (or else the constant gcd of the coefficients could be factored out).
Theorem 45.29. (Continued)

**Theorem. 45.29.** If $D$ is a UFD, then $D[x]$ is a UFD.

**Proof. (Continued)** The factorization of $f(x) \in D[x]$ where $f(x)$ has degree 0 is unique since $D$ is a UFD. If $f(x)$ has degree greater than 0, then any factorization of $f(x)$ into irreducibles in $D[x]$ corresponds to a factorization in $F[x]$ into units (the factors in $D$; the constant factors) and, by Lemma 45.27, irreducible polynomials in $F[x]$. By Theorem 23.20, these irreducible polynomials are unique, except for possible constant factors in $F$. But as an irreducible in $D[x]$, each polynomial of degree $> 0$ appearing in the factorization of $f(x)$ in $D[x]$ is primitive (or else the constant gcd of the coefficients could be factored out).
Theorem. 45.29. If $D$ is a UFD, then $D[x]$ is a UFD.

Proof. (Continued) By the uniqueness part of Lemma 45.23, these irreducible polynomial factors are unique in $D[x]$ up to unit factors (that is, unique up to being associates). The product of the irreducibles in $D$ in the factorization of $f(x)$ (that is, the constant factors) is the content of $f(x)$, which is unique up to a unit factor by Lemma 45.23. Thus all irreducibles in $D[x]$ appearing in the factorization are unique up to order and associates.
Theorem 45.29. If $D$ is a UFD, then $D[x]$ is a UFD.

Proof. (Continued) By the uniqueness part of Lemma 45.23, these irreducible polynomial factors are unique in $D[x]$ up to unit factors (that is, unique up to being associates). The product of the irreducibles in $D$ in the factorization of $f(x)$ (that is, the constant factors) is the content of $f(x)$, which is unique up to a unit factor by Lemma 45.23. Thus all irreducibles in $D[x]$ appearing in the factorization are unique up to order and associates.
Corollary 45.30. If $F$ is a field and $x_1, x_2, \ldots, x_n$ are indeterminates, then $F[x_1, x_2, \ldots, x_n]$ is a UFD.

Proof. By Theorem 23.20, $F[x]$ is a UFD. By Corollary 45.30 and induction, $F[x_1, x_2], F[x_1, x_2, x_3], \ldots, F[x_1, x_2, \ldots, x_n]$ are UFDs.
**Corollary 45.30.** If $F$ is a field and $x_1, x_2, \ldots, x_n$ are indeterminates, then $F[x_1, x_2, \ldots, x_n]$ is a UFD.

**Proof.** By Theorem 23.20, $F[x]$ is a UFD. By Corollary 45.30 and induction, $F[x_1, x_2], F[x_1, x_2, x_3], \ldots, F[x_1, x_2, \ldots, x_n]$ are UFDs. \qed