Assigned reading: Chapters 18, 19, 20 of Gallian.

Assigned questions to hand in:

(1) (Gallian Chapter 18 #2) In an integral domain, show that $a$ and $b$ are associates if and only if \langle a \rangle = \langle b \rangle.

Let $D$ be an integral domain and let $a, b \in D$. First, note that if $a = 0$, then its only associate is itself. Therefore, we can assume $a \neq 0, b \neq 0$.

We prove the two directions of implication. First, suppose $a$ and $b$ are associates. Then there is a unit $u \in D$ such that $a = ub$. We want to show that \langle a \rangle = \langle b \rangle. Let $x \in \langle a \rangle$. Then there is $r \in D$ such that $x = ar$. Substituting $b$ for $a$: $x = (ub)r = b(ur)$. Thus, $x \in \langle b \rangle$. For the reverse subset inclusion, let $y \in \langle b \rangle$. Then there is $s \in D$ such that $y = bs$. Substituting $a$ for $b$: $y = (a^{-1}s)b = (a^{-1}s)a$. Thus, $y \in \langle a \rangle$.

For the other direction, suppose \langle a \rangle = \langle b \rangle. We want to show that $a$ and $b$ are associates. Since $a \in \langle a \rangle = \langle b \rangle$, there is some $r \in D$ such that $a = br$. Since $b \in \langle b \rangle = \langle a \rangle$, there is some $s \in D$ such that $b = as$. Substituting for $b$ in the first equation using the second:

$$a = br = (as)r = a(sr).$$

Since $a \neq 0$ and $D$ is a integral domain, we can cancel to get

$$1 = sr.$$ 

In particular, this says that $s, r$ are each units. Hence, $a, b$ are associates.

(2) (Gallian Chapter 18 #4) In an integral domain, show that the product of an irreducible and a unit is an irreducible.

Solution: Let $D$ be an integral domain and let $a$ be irreducible and $u$ be a unit. We want to show that $au$ is irreducible.

- Is $au$ nonzero and nonunit?
  
  Since $a$ is irreducible, it is is nonzero and not a unit. Also, $u$ is nonzero because it is a unit. Therefore, since $D$ is an integral domain (so has no zero divisors), $au$ is nonzero. Suppose, towards a contradiction that $au$ is a unit. Let $y$ be such that $1 = (au)y$. By associativity, $1 = a(uy)$, contradicting the assumption that $a$ is not a unit.

- Does $au$ not have any nontrivial factorizations?
  
  Suppose $b, c \in D$ are such that $au = bc$. We want to show that either $b$ is a unit or $c$ is a unit. Since $u$ is a unit, we can multiply both sides by $u^{-1}$:

$$a = bcu^{-1} = b(cu^{-1}).$$

By assumption, $a$ is irreducible. Hence, either $b$ is a unit or $cu^{-1}$ is a unit. If $b$ is a unit, we’re done. Otherwise $cu^{-1}$ is a unit, and let $z \in D$ be such that $1 = (cu^{-1})z$. By associativity, $1 = c(u^{-1}z)$ and $c$ is a unit, as required.
(3) (Gallian Chapter 18 #24) Let $F$ be a field. Show that in $F[x]$, a prime ideal is a maximal ideal.

Solution: Let $F$ be a field and let $I \subseteq F[x]$ be a prime ideal. Assume $I$ is not trivial. Since $F[x]$ is a PID, there is some $a(x) \in F[x]$ such that $I = \langle a(x) \rangle$. We will prove that $a(x)$ is prime. First, note that a prime ideal is a proper ideal; hence, $a(x)$ is not a unit. Moreover, by assumption, $a(x) \neq 0$. Suppose $b(x), c(x) \in F[x]$ are such that $a(x)|b(x)c(x)$. We want to show that $a(x)|b(x)$ or $a(x)|c(x)$. By definition of divisibility, there is some $r(x) \in F[x]$ such that $b(x)c(x) = a(x)r(x)$. By definition of principal ideals, this means that $b(x)c(x) \in \langle a(x) \rangle = I$. Since $I$ is prime, either $b(x) \in I$ or $c(x) \in I$. In the first case, $a(x)|b(x)$; in the second case, $a(x)|c(x)$. Thus, $a(x)$ is prime.

By Theorem 18.2, since $F[x]$ is a PID and $a(x)$ is prime, $a(x)$ is irreducible. By Theorem 17.5, this implies that $I = \langle a(x) \rangle$ is a maximal ideal in $F[x]$.

(4) (Gallian Chapter 20 #4) Find the splitting field of $x^4 + 1$ over $\mathbb{Q}$.

Solution: We factor the polynomial in $\mathbb{C}$:

$$x^4 + 1 = (x^2 - i)(x^2 + i) = (x + \sqrt{i})(x - \sqrt{i})(x + \sqrt{-i})(x - \sqrt{-i}).$$

Therefore, the splitting field is

$$\mathbb{Q}(\pm \sqrt{i}, \pm \sqrt{-i}) = \mathbb{Q}(\sqrt{i}, \sqrt{-i}).$$

In fact, we can say even more. Recall the polar notation for complex numbers:

$$i = e^{\frac{\pi i}{2}}, \quad -i = e^{\frac{-\pi i}{2}}$$

so

$$\sqrt{i} = e^{\frac{2\pi i}{8}} = e^{\frac{\pi i}{4}}, \quad \sqrt{-i} = e^{\frac{-2\pi i}{8}} = e^{\frac{-\pi i}{4}}.$$ 

In particular, $\sqrt{-i}$ is a power (the seventh power) of $\sqrt{i}$. Hence,

$$\mathbb{Q}(\sqrt{i}, \sqrt{-i}) = \mathbb{Q}(\sqrt{i}).$$

(5) (Gallian Chapter 20 #6) Let $a, b \in \mathbb{R}$, with $b \neq 0$. Show that $\mathbb{R}(a + bi) = \mathbb{C}$.

Solution: Since $a + bi \in \mathbb{C}$, an extension field of $\mathbb{R}$, $\mathbb{R}(a + bi)$ is the smallest subfield of $\mathbb{C}$ that contains $a + bi$. Therefore, by definition, $\mathbb{R}(a + bi) \subseteq \mathbb{C}$. We will show the subset inclusion in the reverse direction. Let $z \in \mathbb{C}$. By definition of the complex numbers, there are $x, y \in \mathbb{R}$ such that $z = x + iy$. Note that $\mathbb{R} \subseteq \mathbb{R}(a + bi)$ by definition. Therefore,

$$x \in \mathbb{R}(a + bi), \quad y \in \mathbb{R}(a + bi)$$

and also

$$a \in \mathbb{R}(a + bi), \quad b \in \mathbb{R}(a + bi).$$

Also, $a + bi \in \mathbb{R}(a + bi)$. Since $\mathbb{R}(a + bi)$ is a field, it is closed under subtraction. Thus, $bi = (a + bi) - a \in \mathbb{R}(a + bi)$. Moreover, $\mathbb{R}(a + bi)$ is closed under division by nonzero elements. Since $b \neq 0$, $i = b^{-1}(bi) \in \mathbb{R}(a + bi)$. By closure of $\mathbb{R}(a + bi)$ under multiplication, $iy \in \mathbb{R}(a + bi)$. By closure under addition, $x + iy \in \mathbb{R}(a + bi)$, as required to prove that $\mathbb{C} \subseteq \mathbb{R}(a + bi)$. 

Let $F$ be a field and let $a, b \in F$ with $a \neq 0$. If $c$ belongs to some extension of $F$, prove that $F(c) = F(ac + b)$.

**Solution:** Let $E$ be an extension field of $F$ containing $c$. By closure under addition and multiplication, $E$ contains $ac + b$ as well. Thus, $E$ is an extension field of both $F(c)$ and $F(ac + b)$. By exercise #35, for any $d \in E$, $F(d)$ is the intersection of all subfields of $E$ that contain $d$. We will show that $ac + b \in F(c)$ and hence $F(c)$ is a subfield of $E$ containing $ac + b$: $F(ac + b) \subseteq F(c)$. Similarly, we will show that $c \in F(ac + b)$ and hence $F(ac + b)$ is a subfield of $E$ containing $c$: $F(c) \subseteq F(ac + b)$.

- **WTS** $ac + b \in F(c)$: Since $F \subseteq F(c)$ and $a, b \in F$, $a, b \in F(c)$. Also, by definition of $F(c)$, $c \in F(c)$. By closure of $F(c)$ under addition and multiplication, $ac + b \in F(c)$. ✓

- **WTS** $c \in F(ac + b)$: Since $F \subseteq F(ac + b)$ and $a, b \in F$, $a, b \in F(c)$. Also, $ac + b \in F(ac + b)$. By closure of $F(ac + b)$ under subtraction: $ac = (ac + b) - b \in F(ac + b)$. Since $a \neq 0$, $a^{-1} \in F \subseteq F(ac + b)$. By closure of $F(ac + b)$ under multiplication, $c = a^{-1}(ac) \in F(ac + b)$. ✓