HW 4

1a when $I = \{0\}$, I is the ideal generated by the zero polynomial.

If I contains a nonzero constant polynomial, say $a \in F$, then $\frac{1}{a} \cdot a \in I$, so $1 \in I$, so $I = R$ is the ideal generated by 1.

b. If I does contain a nonzero polynomial and does not contain any nonzero constant polynomials, then let $f(x) \in I$ be a polynomial of smallest degree in I. By assumption, $\deg(f(x)) \geq 1$. we know $(f(x)) \subseteq I$. We want to prove $\supseteq$.

Let $g(x) \in I$. by the division alg, $\exists\ q(x), r(x) \in F[x]$ with
$$g(x) = q(x) f(x) + r(x),$$ and either $r(x) = 0$ or $\deg(r(x)) < \deg(f(x))$.

But $g(x) - q(x) f(x) = r(x)$, and $LHS \in I \Rightarrow r(x) \in I$.

so if $r(x) \neq 0$ we get a contradiction of the assumption that $f(x)$ has minimal degree. So $g(x) = q(x) f(x)$.

And so $I = (f(x))$.

so $r(x) = 0$ and $g(x) = q(x) f(x)$,

so $g(x) \in (f(x))$,

so $I = (f(x))$.

2. a. $\Longrightarrow$ Assume R is noetherian.

then let

$I_1 \subseteq I_2 \subseteq \dots$ be an ascending

chain of ideals.

Let $J = \bigcup_{i=1}^{\infty} I_i$.

① $0 \in J$, since $0 \in I_1$

② $\forall\, a, b \in J$, $\exists\, I_n$ with $a, b \in I_n$,

(if $a \in I_i$, $b \in I_j$, let $n = \max(i, j)$).

so $a + b \in I_n$, so $a + b \in J$.

③ $\forall\, a \in J$, $\exists\, I_n$ with $a \in I_n$. so $r \cdot a \in I_n$

for any $r \in R$.

Hence J is an ideal in R.

by assumption, $J = (a_1, a_2, \dots a_d)$ for

some $a_1 \dots a_d \in R$.

say $a_1 \in I_{n_1}$, $a_2 \in I_{n_2}$ ... $a_d \in I_{n_d}$.

Let $n = \max\{n_1, \dots, n_d\}$.

then $a_1 \dots a_d \in I_n$.

$$\Rightarrow \quad (a_1, \dots, a_d) \subseteq I_n \subseteq J$$

$$\Rightarrow \quad J \subseteq I_n \subseteq J$$

$$\Rightarrow \quad I_n = J.$$

but, $a_1, \dots, a_d \in I_N$ for any $N \geq n$.

so the same argument implies

$$I_N = J \text{ for } N \geq n.$$

So $I_n = I_{n+1} = I_{n+2} = \dots$

So R has no <u>infinite</u> ascending chains.

$\Leftarrow$ We will show that if R is not noetherian, then R has an infinite ascending chain.

Let $I \subseteq R$ be an ideal which is not finitely generated.

pick $a_1 \in I$. by assumption, $(a_1) \subsetneq I$.

pick $a_2 \in I \setminus (a_1)$. by assumption

$$(a_1) \subsetneq (a_1, a_2) \subsetneq I.$$

continuing in this way, we construct a chain

$$(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \cdots \subsetneq (a_1, \ldots a_n) \subsetneq \cdots$$

which is infinite (since $(a_1, \ldots, a_n)$ is always a proper subideal of I, we can always pick $a_{n+1} \in I \setminus (a_1, \ldots, a_n)$), and where each containment is proper. So R has an infinite ascending chain.

b. $\Longrightarrow$ if R is noetherian, consider S a nonempty set of ideals. There are two cases:

① if S is finite, pick some $I \in S$.
if there's no bigger ideal in S, then I is maximal.
If $\exists\ J \in S$, $I \subsetneq J$, then consider J.

the set of elements bigger than J_7 is smaller than the set of elements bigger than I, so we can continue taking larger ideals a finite number of times until we find a max.

if S is infinite, consider a chain in S,

$I_1 \subseteq \dots \subseteq I_n \subseteq \dots$

since R is noetherian we know $\exists N$

with $I_N = I_{N+1} = \dots$

so this chain has an upper bound <u>in</u> S.

Zorn $\Rightarrow$ S has a maximal element.

$\Leftarrow$ Suppose every nonempty collection S of ideals (in S) has a maximal element. Then consider a chain $I_1 \subseteq \dots \subseteq I_n \subseteq \dots$.

Let I_k be the upper bound of this chain.

so $I_k \supseteq I_n \quad \forall n \in \mathbb{N}$

but also $I_k \subseteq I_{k+1} \subseteq I_{k+2} \subseteq \dots$ in the chain.

so $I_k = I_{k+1} = I_{k+2} = \dots$

so every chain stabilizes, and by problem 2a, that implies R is noetherian.

3. ψ is defined by $\psi(a+b\sqrt{2}) = a - b\sqrt{2}$.

ψ is injective because if $a-b\sqrt{2} = c - d\sqrt{2}$

then $(a-c) - (b-d)\sqrt{2} = 0$, and

since $\{1, \sqrt{2}\}$ is a $\mathbb{Q}$-basis, this

means $\begin{array}{l} a-c=0 \\ b-d=0 \end{array}$ so $a=c$, $b=d$.

ψ is surjective because for any $a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$,

$\psi(a-b\sqrt{2}) = a+b\sqrt{2}$.

$\psi(0+0\sqrt{2}) = 0-0\sqrt{2}$ (sends 0 to 0)

$\psi(1+0\sqrt{2}) = 1-0\sqrt{2}$ (sends 1 to 1).

$\psi((a+b\sqrt{2})(c+d\sqrt{2}))$

$= \psi((ac+2bd)+(ad+bc)\sqrt{2})$

$= (ac+2bd) - (ad+bc)\sqrt{2}$.

$= (a-b\sqrt{2})(c-d\sqrt{2})$

$= \psi(a+b\sqrt{2})\psi(c+d\sqrt{2})$.

$\psi(a+b\sqrt{2}+c+d\sqrt{2})$

$= \psi((a+c)+(b+d)\sqrt{2})$

$= (a+c)-(b+d)\sqrt{2}$

$= (a-b\sqrt{2})+(c-d\sqrt{2})$

$= \psi(a+b\sqrt{2})+\psi(c+d\sqrt{2})$.

So ψ is an isomorphism $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$.

b. $r \in \mathbb{Q}$ can be written as an elt of $\mathbb{Q}(\sqrt{2})$ in exactly one way: $r + 0\sqrt{2}$.

$\psi(r+0\sqrt{2}) = r - 0\sqrt{2} = r + 0\sqrt{2}$.

so ψ fixes $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$.

c. If $\xi : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$ is any automorphism fixing $\mathbb{Q}$, then $\xi(\sqrt{2})$ is a conjugate of $\sqrt{2}$. so $\xi(\sqrt{2}) = \pm\sqrt{2}$

And we know $\xi(1)=1$ since ξ fixes $\mathbb{Q}$.

If $\xi(1) = 1$ and $\xi(\sqrt{2}) = \sqrt{2}$

then $\xi(a+b\sqrt{2}) = a+b\sqrt{2} \ \forall \ a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

so ξ is the identity function.

If $\xi(1) = 1$ and $\xi(\sqrt{2}) = -\sqrt{2}$ then

$\xi(a+b\sqrt{2}) = a - b\sqrt{2}$ is the automorphism

ψ from above.

4 $\quad \alpha = \sqrt{1+\sqrt{2}}$

$$\alpha^2 = 1+\sqrt{2}$$

$$\alpha^2 - 1 = \sqrt{2}$$

$$(\alpha^2-1)^2 = 2$$

$$(\alpha^2-1)^2 - 2 = 0.$$

$$\alpha^4 - 2\alpha^2 - 1 = 0$$

so $x^4 - 2x^2 - 1$ is the min. poly. of α.

QF $\Rightarrow$

$$x^2 = \frac{2 \pm \sqrt{4-4(1)(-1)}}{2}$$

$$x^2 = \frac{2 \pm \sqrt{8}}{2}$$

$$x^2 = \frac{2 \pm 2\sqrt{2}}{2} = 1 \pm \sqrt{2}$$

$$\Rightarrow \quad x = \pm\sqrt{1 \pm \sqrt{2}}$$

are the four conjugates of α.

5. Let $G(E/F)$ = the set of all automorphisms of E that fix F.

if $\sigma, \tau \in G(E/F)$ then:

$\sigma \circ \tau$ is still an isomorphism $E \longrightarrow E$,

and $\sigma \circ \tau(a) = \sigma(\tau(a)) = \sigma(a) = a$
$\forall a \in F$.

so $G(E/F)$ is closed under composition.

if σ is an isomorphism $E \to E$ fixing F, then $\sigma^{-1} : E \to E$ is also an isomorphism fixing F.

So $G(E/F)$ has inverses, and the identity function $\mathrm{id} : E \to E$ is the identity element.

composition of functions is associative.

So $G(E/F)$ is a group.

we saw in Q3 that $G(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ has two elements, $\{\mathrm{id}, \psi\}$. the group multiplication table is

	id	ψ
id	id	ψ
ψ	ψ	ψ

this group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. (cyclic, order 2).