Section 3.2

1. (Problem 19) Prove $\mathbf{Q}(\sqrt{2})$ is the smallest subfield of $\mathbf{R}$ containing $\sqrt{2}$.

> **Solution:** We must show that if F is a subfield of $\mathbf{R}$ containing $\sqrt{2}$ then $\mathbf{Q}(\sqrt{2}) \subseteq F$; let F be such a field. Prove that because F contains 1 (part of the definition of subfield) and is closed under addition/additive inverses, F must contain all of $\mathbf{Z}$. Then prove that because F must contain inverses of nonzero elements, it follows that F contains all of $\mathbf{Q}$. Now because F contains $\sqrt{2}$ and is closed under multiplication, it must contain elements of the form $b\sqrt{2}$ where $b \in \mathbf{Q}$. Finally, since it is closed under addition, we conclude F contains all elements of the form $a + b\sqrt{2}$ where $a, b \in \mathbf{Q}$, i.e. F contains $\mathbf{Q}(\sqrt{2})$.

2. (Problem 25) Let R be an integral domain and $Q \supseteq R$ be its field of quotients. Prove if $\sigma : R \to R$ is a (ring) automorphism, then there is a unique automorphism $\bar{\sigma} : Q \to Q$ extending σ, i.e. satisfying $\bar{\sigma}(r) = \sigma(r)$ for all $r \in R$.

> **Solution:** We can define $\bar{\sigma} : Q \to Q$ by $\bar{\sigma}(\frac{r}{u}) = \frac{\sigma(r)}{\sigma(u)}$ (notice that $u \neq 0 \implies \sigma(u) \neq 0$ by injectivity of σ). One verifies that this is a ring automorphism, for instance the calculation
>
> $$\begin{aligned}\bar{\sigma}(\frac{r}{u} + \frac{s}{v}) &= \bar{\sigma}(\frac{rv + su}{uv}) = \frac{\sigma(rv + su)}{\sigma(uv)} \\ &= \frac{\sigma(r)\sigma(v) + \sigma(s)\sigma(u)}{\sigma(u)\sigma(v)} = \frac{\sigma(r)}{\sigma(u)} + \frac{\sigma(s)}{\sigma(v)} \\ &= \bar{\sigma}(\frac{r}{u}) + \bar{\sigma}(\frac{s}{v})\end{aligned}$$
>
> proves additivity.
>
> For uniqueness, suppose $\varphi : Q \to Q$ is another automorphism satisfying $\varphi(r) = \sigma(r)$ for all $r \in R$. Since $\varphi(1) = 1$ (this is an axiom of ring homomorphisms), by multiplicativity we can calculate for any $r \in R$
>
> $$1 = \varphi(1) = \varphi(r \cdot \frac{1}{r}) = \varphi(r)\varphi(\frac{1}{r}),$$
>
> and from this we conclude that $\varphi(\frac{1}{r}) = \frac{1}{\varphi(r)}$. But then using multicativity again, along with the fact that $\varphi(a) = \sigma(a)$ for all $a \in R$, we calculate that for any element $\frac{r}{u} \in Q$,
>
> $$\varphi(\frac{r}{u}) = \varphi(r \cdot \frac{1}{u}) = \varphi(r)\varphi(\frac{1}{u}) = \varphi(r)\frac{1}{\varphi(u)} = \frac{\varphi(r)}{\varphi(u)} = \frac{\sigma(r)}{\sigma(u)} = \bar{\sigma}(\frac{r}{u}),$$
>
> and thus we conclude $\varphi = \bar{\sigma}$, proving uniqueness.

Section 3.3

3. (Problem 5)

   (a) If A is an ideal of R and B is an ideal of S, prove $A \times B$ is an ideal of $R \times S$.

   Solution: If $(a, b) \in A \times B$ and $(r, s) \in R \times S$, then $(a, b)(r, s) = (ar, bs)$ which is an element of $A \times B$ since $ar \in A$ and $bs \in B$ (since A and B are ideals). Similarly $(r, s)(a, b) \in A \times B$; checking it's an additive subgroup is equally straightforward.

   (b) Prove every ideal of $R \times S$ is of the form $A \times B$ as in (a).

   Solution: Let I be an ideal of $R \times S$; let $A = \{a \in R \mid (a, 0) \in I\}$ and $B = \{b \in S \mid (0, b) \in I\}$. One does the straightfoward verification that A and B are ideals, and we claim $I = A \times B$.

   On one hand if $(a, b) \in A \times B$ then $a \in A$ implies $(a, 0) \in I$ and $b \in B$ implies $(0, b) \in I$, and closure under addition then implies $(a, b) \in I$. In the other direction, if $(a, b) \in I$, then multiplying by $(1, 0)$ we deduce $(a, 0) \in I$ and hence deduce $a \in A$; similarly $b \in B$ so $(a, b) \in A \times B$, completing the proof of equality.

4. (Problem 9) Let $R = \mathbf{Z}[i]$ and in each of the following cases find the number of elements in R/A, and describe the cosets.

   (a) $A = Ri$,

   (b) $A = R(1 - i)$,

Solution: I will write (i) or $(1 - i)$ instead of Ri or $R(1 - i)$, etc. For part (a), just notice that i is a unit in R, so $(i) = R$ and then $R/A = 0$ (i.e. there is one element of R/A).

For part (b), notice that because $(1 - i) + A = 0 + A$, we deduce $i + A = 1 + A$, and therefore for any $a + bi \in R$ we have $(a + bi) + A = (a + b) + A$. Now notice that $2 \in A = (1 - i)$ because $2 = (1 + i)(1 - i)$. Using this, notice that if a and b have the same parity (i.e. they are either both even or both odd), then $a + b$ is even so for some $k \in \mathbf{Z}$ we have $a + b = 2k \in A$ (since $2 \in A$ and A is an ideal), and thus we deduce that $(a + b) + A = 0 + A$, and hence $(a + bi) + A = 0 + A$.

On the other hand, if a and b have different parities then $a + b$ is odd, so if $a + b = 2k + 1$ for $k \in \mathbf{Z}$ then we see using similar logic to above that $(a + b) + A = 1 + A$, and hence $(a + bi) + A = 1 + A$.

Thus we see we have at most two cosets, $0 + A$ and $1 + A$, and we claim these are distinct; these are the same coset if and only if $1 \in A$, which is the case if and only if $R = A = (1 - i)$, which is the case if and only if $1 - i$ is a unit in R; but $1 - i$ is not a unit in R because have the multiplicative norm map $N : R \to \mathbf{Z}$ defined previously, and using multiplicativity we see that if $1 - i$ is a unit then we could conclude $N(1 - i) = \pm 1$, but direct calculation shows $N(1 - i) = 2$.