Michaelmas 2012, NT III/IV, Problem Sheet 3.

1. Let $J = (2, 1+\sqrt{-3})_R$ where $R = \mathbb{Z}[\sqrt{-3}]$. Show that
   (i) the map $f : R \to \mathbb{Z}_2$, defined by $f(a+b\sqrt{-3}) = a+b \mod 2$, is a ring homomorphism with kernel J. Deduce that J is a maximal ideal of R.
   (ii) $J^2 = (2)_R J$ yet $J \neq (2)_R$. ⟦This shows that we cannot always just "cancel" factors in products of ideals.⟧
   (iii) if $\alpha \in R$ is such that $\alpha J \subseteq (2)_R$ then $\alpha \in J$.
   (iv) with the obvious definition of an ideal being divisible by another, J does *not* divide $(2)_R$ even though $J \supseteq (2)_R$.

2. (a) Let d be a positive integer such that $\sqrt{d} \notin \mathbb{Q}$. Let $R = \mathbb{Z}[\sqrt{d}]$ and define the map $\varphi : R \to \mathbb{Z}$ by $\varphi(a+b\sqrt{d}) = |a^2 - db^2|$ (for $a, b \in \mathbb{Z}$). Show that φ satisfies the following three conditions:
      (i) φ is multiplicative, i.e., $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$;
      (ii) $\varphi(\alpha) = 0 \quad \Rightarrow \quad \alpha = 0$;
      (iii) $\varphi(\alpha) = 1 \quad \Rightarrow \quad \alpha \in R^*$ (i.e., α is a unit).
   (b) Show that a function which satisfies the above three conditions (i)—(iii) also satisfies the following
   $$\forall \beta, \gamma \in R \setminus \{0\} \text{ and } \beta \notin R^* \quad \text{we have} \quad \varphi(\beta\gamma) > \varphi(\gamma)\,. \tag{1}$$
   (c) Show that in an integral domain, in which (1) holds, every element can be factorised into irreducibles.

3. Show that φ is a Euclidean norm on R in the following cases
   (a) (i) $R = \mathbb{Q}[X]$, $\varphi(f(X)) = \deg(f(X))$ if $f(X) \neq 0$;
      (ii) $R = \mathbb{Z}[i]$, $\varphi(\alpha) = |\alpha|^2$;
      (iii) $R = \mathbb{Z}[\sqrt{3}]$, $\varphi(a+b\sqrt{3}) = |a^2 - 3b^2|$ if a and $b \in \mathbb{Z}$.
   (b) With R and φ as in the corresponding part of (a), find a $\gamma \in R$ such that $\varphi(\beta - \alpha\gamma) < \varphi(\alpha)$ where
      (i) $\alpha = X^3 - 1$, $\beta = X^4 + X^2 + 6$;
      (ii) $\alpha = 4 + 5i$, $\beta = 15 + 8i$;
      (iii) $\alpha = 1 + 3\sqrt{3}$, $\beta = 5 - 9\sqrt{3}$.

4. Let R be the subring $\{\sum_{j=1}^{s} a_j 2^{r_j} \mid s \in \mathbb{Z}^{>0},\ r_j \in \mathbb{Q}^{\geq 0},\ a_j \in \mathbb{Z}\}$ of $\mathbb{R}$ and let P be its subgroup $\{\sum_{j=1}^{s} a_j 2^{r_j} \mid s \in \mathbb{Z}^{>0},\ r_j \in \mathbb{Q}^{>0},\ a_j \in \mathbb{Z}\}$. Show that
   (i) $P^2 = P$,
   (ii) P is a maximal ideal of R and
   (iii) $R = P \cup (1 + P)$.

5. Using the first isomorphism theorem for rings from Algebra II, or otherwise, show that $\mathbb{Q}[\sqrt{5}]$ is a field isomorphic to $\mathbb{Q}[X]/(X^2 - 5)$.

6. Let F be an extension of a field K with basis $\{\gamma_1, \ldots, \gamma_n\}$ over K.
   Show that, for any $\gamma \in F^*$, $\{\gamma\gamma_1, \ldots, \gamma\gamma_n\}$ is also a K-basis for F.

7. Let α be an (irrational) algebraic number and let a, b, c and d be rational numbers such that $ad \neq bc$. Show that $\mathbb{Q}[(a\alpha + b)/(c\alpha + d)] = \mathbb{Q}[\alpha]$.

8. Let K be an extension of $\mathbb{Q}$ of prime degree p and suppose that $\alpha \in K \setminus \mathbb{Q}$. Use the Tower Theorem to show that $|\mathbb{Q}[\alpha] : \mathbb{Q}| = p$ (and hence that $K = \mathbb{Q}[\alpha]$).

9. Find $|\mathbb{Q}[\alpha] : \mathbb{Q}|$ when α is (i) $\sqrt{7}$ (ii) $\sqrt[3]{5} + 2$, (iii) $e^{2\pi i/5}$ (a fifth root of 1).

10. Let p and q be coprime integers, where p is not a square. Show that the minimum polynomial of $\sqrt{p}$ over $\mathbb{Q}[\sqrt{q}]$ is $X^2 - p$.