This solution set was written by Pokman; Ravi has added some comments and hopefully hasn’t introduced too many errors!

1. Show that a ring in which all ideals are finitely generated cannot have an infinite sequence of ideals

\[ I_1 \subset I_2 \subset I_3 \subset \ldots \]

Conversely, show that if a ring has no infinite sequence of ideals, then all ideals are finitely generated.

Solution. Suppose all ideals of a ring \( R \) are finitely generated, and we have an increasing sequence of ideals, \( I_1 \subset I_2 \subset I_3 \subset \ldots \). The union \( I = \bigcup_{i \geq 1} I_i \) is also an ideal. (Not true for any union of ideals. The sequence being increasing is important.) By assumption, \( I = (a_1, \ldots, a_n) \) is finitely generated. Since the sequence \( \{I_k\}_{k \geq 1} \) is increasing, all \( a_i \) are contained in \( I_N \) whenever \( N \) is big enough, which implies \( I = (a_1, \ldots, a_n) \subset I_N \subset I \Rightarrow I_N = I \) for all sufficiently large \( N \). Hence, the increasing sequence of ideals stabilizes after a finite number of steps.

Conversely, suppose \( R \) satisfies the ascending chain condition on its ideals, and let \( I \) be an ideal of \( R \). Choose a sequence of ideals inductively as follows: Pick some \( a_1 \in I \) and let \( I_1 = (a_1) \). Suppose \( I_n = (a_1, \ldots, a_n) \subset I \) has been chosen. If \( I_n \subset I \), pick some \( a_{n+1} \in I - I_n \), and let \( I_{n+1} = I_n + (a_{n+1}) \subset I \). Note that \( I_n \subset I_{n+1} \). By assumption, this procedure must terminate after a finite number of steps, which happens only when \( I = I_n = (a_1, \ldots, a_n) \). Hence any ideal is finitely generated.

(You can’t start with: let \( (a_1, a_2, \ldots, ) \) be a generating set. Do you see why? How do you know there is a countable generating set? Another common mistake is talk about “the” generating set.)

2. (a) Show that if \( n \neq 4 \), the only normal subgroups of \( S_n \) are \( \{e\} \), \( A_n \), and \( S_n \).
(b) Describe all group homomorphisms from \( S_7 \rightarrow S_6 \).

Solution. (a) The cases \( n = 2, 3 \) are easily checked. Consider \( n \geq 5 \). Let \( N \) be a normal subgroup of \( S_n \). Then \( N \cap A_n \) is a normal subgroup of \( A_n \). Since \( A_n \) is simple, \( N \cap A_n \) must equal \( \{e\} \) or \( A_n \). In the latter case, \( N \supset A_n \). As \( |S_n : A_n| = 2 \), the only subgroups of \( S_n \) containing \( A_n \) are \( A_n \) and \( S_n \), and both of them are normal.

Date: Thursday, November 7, 2002.
Suppose $N \cap A_n = \{e\}$. Assume $N \neq \{e\}$ and let $\sigma, \tau \in N - \{e\}$. Since $\sigma, \tau \notin A_n$, they are odd permutations. Since the product of two odd permutations is even, $A_n$ consists of all even permutations and $N \cap A_n = \{e\}$, we have $\sigma^2 = e = \sigma \tau$, which implies $\sigma = \tau$. Hence $N$ contains at most one nontrivial element. [This is a proof of problem 2.95(i) in Rotman.] However, since $N$ is normal, whenever $N$ contains an element, $N$ contains all its conjugates, and the conjugacy class of any nontrivial element of $S_n$ consists of more than one elements (true for any $n > 2$). Thus $N$ cannot contain exactly one nontrivial element. We conclude $N = \{e\}$.

(b) Let $\varphi : S_7 \to S_5$ be a homomorphism. By (a), $\ker \varphi = \{e\}$, $A_7$ or $S_7$. The first case is impossible since $|S_7| > |S_5|$. If $\ker \varphi = A_7$, we must have $\im \varphi = \{e, \tau\}$, where $\tau \in S_5$ is of order 2. Conversely, for any such $\tau$, since $S_7/A_7 \cong \{e, \tau\}$, there exists a homomorphism with $A_7$ as the kernel and $\{e, \tau\}$ as the image. Finally, we have $\ker \varphi = S_7$ if and only if $\varphi$ maps all elements of $S_7$ to $e \in S_5$.

3. Prove that every nonzero prime ideal in a Principal Ideal Domain is a maximal ideal.

Solution. Let $(p) \neq (0)$ be prime and $(a) \supseteq (p)$. Since $p \in (a)$, we have $p = ab$ for some $b \in R$. Then $ab \in (p)$ but $a \notin (p)$ implies $b \in (p)$, or $b = cp$ for some $c \in R$. Hence we have $p = ab = acp \Rightarrow 1 = ac$, since $R$ is a domain and $p \neq 0$. Therefore, $a$ is a unit and $(a)$ is the whole ring. This proves $(p)$ is maximal.

(Many people never explicitly used the fact that $(p) \neq (0)$. It is necessary — do you see where?)

4.

(a) Note that $\omega = \frac{-1 + \sqrt{-3}}{2}$ is a cube root of 1, and $\omega^2 + \omega + 1 = 0$. Prove that the subset $\{x + y\omega \in \mathbb{Z}[\omega] : x + y \text{ is divisible by } 3\} \subset \mathbb{Z}[\omega]$ is an ideal. Is it prime?.

(b) Describe the set of integers of the form $a^2 - ab + b^2$ (a, b integers).

Solution. (a) Let $I$ be the subset defined in the question. It is straightforward to directly check that $I$ is an ideal. Instead, observe that the following are equivalent:

\[(i) \: 3|a + b, \quad (ii) \: 3|N(a + b\omega), \quad (iii) \: a + b\omega \in (1 - \omega).\]

(i) \iff (ii): since $N(a + b\omega) = a^2 - ab + b^2 = (a + b)^2 - 3ab$. (iii) \implies (ii): since $N(1 - \omega) = 3$. (i) \implies (iii): since $a + b\omega = a + b - b(1 - \omega) = (1 - \omega) \frac{a + b}{3} (1 - \omega) - b$. Hence by (iii), $I = (1 - \omega)$ is an ideal. Also, (ii) implies $I$ is prime: $3|N(\alpha\beta) = N(\alpha)N(\beta) \Rightarrow 3|N(\alpha)$ or $3|N(\beta)$.

(b) We first determine when a prime integer $p$ can be so expressed. If $p = a^2 - ab + b^2$, by reducing to mod 3, it is easy to see that we must have $p \equiv 0, 1(\text{mod } 3)$. Conversely, if $p = 3$, take $a = 1, b = -1$. If $3|p - 1$, by Theorem 2.78 in Rotman, there exists $\tau \in \mathbb{F}_p^\times$ of order 3. Hence we have $(\tau^2 + \tau + 1) = \tau^3 - 1 = 0$ but $\tau - 1 \neq 0$, thus $\tau^2 + \tau + 1 = 0$. This means there exist $t \in \mathbb{Z}$ such that $t^2 + t + 1 = pk$ for some $k \in \mathbb{Z}$. 

2
In particular, we may require $1 < t \leq p - 1$, so that

$$0 < pk = t^2 + t + 1 = \left( t + \frac{1}{2} \right)^2 + \frac{3}{4} \leq \left( p - \frac{1}{2} \right)^2 + \frac{3}{4} = p^2 - p + 1 < p^2,$$

and therefore $0 < k < p$. In $\mathbb{Z}[[\omega]]$, we have

$$p \mid pk = t^2 + t + 1 = (t - \omega)(t - \bar{\omega}).$$

Since $\mathbb{Z}[[\omega]]$ is a UFD, some (nonunit) irreducible factor $\alpha$ of $p$ must divide, say, $t - \omega$. Then, $N(\alpha)$ divides both $N(p) = p^2$ and $N(t - \omega) = pk$. Since $0 < k < p$ and $N(\alpha) \neq 1$, we conclude $N(\alpha) = p$. Let $\alpha = a + b\omega$. We then have $p = a^2 - ab + b^2$. Therefore, $p$ can be expressed in the desired form if and only if $p \equiv 0, 1(\text{mod } 3)$.

Alternatively, here is a little more concise proof, paralleling our proof of which numbers are expressible as the sum of two squares: If $p \neq 3$,

$$p = a^2 - ab + b^2 = (a + b\omega)(a + b\bar{\omega})$$

$$\Leftrightarrow (p) \subset \mathbb{Z}[[\omega]] \text{ is not prime}$$

$$\Leftrightarrow \mathbb{Z}[[\omega]]/(p) \cong \mathbb{Z}[x]/(x^2 + x + 1, p) \cong \mathbb{F}_p[x]/(x^2 + x + 1) \text{ has zerodivisors}$$

$$\Leftrightarrow x^2 + x + 1 \text{ is reducible over } \mathbb{F}_p$$

$$\Leftrightarrow \tau^3 = 1 \text{ for some } \tau \in \mathbb{F}_p^* - \{1\} \; (\text{since } p \neq 3)$$

$$\Leftrightarrow 3 \mid p - 1 \; (\text{since } \mathbb{F}_p^* \text{ is cyclic of order } p - 1)$$

Let $S = \{ q \text{ a prime integer } : q \equiv 2(\text{mod } 3) \}$. Suppose $n = a^2 - ab + b^2 = (a + b\omega)(a + b\bar{\omega})$ and $q \in S$ divides $n$. Since $q$ stays irreducible in $\mathbb{Z}[[\omega]]$, we must have, say, $q|a + b\omega$, which implies $q^2 = N(q)|N(a + b\omega) = n$. Then, if we let $n = q^2n', a + b\omega = q(a' + b'\omega)$, we have $n' = (a' + b'\omega)(a' + b'\bar{\omega})$. By the above argument, if $q|n'$, then $q^2|n'$. Therefore, every $q \in S$ divides $n$ exactly an even number of times. Conversely, suppose

$$n = \prod_{p \notin S} p_i^{k_i} \prod_{q_j \in S} q_j^{2l_j}$$

is the prime factorization in $\mathbb{Z}$. Since for any $p_i \notin S$, we have $p_i = N(\alpha_i)$ for some $\alpha_i \in \mathbb{Z}[[\omega]]$, we have

$$n = \prod_i N(\alpha_i)^{k_i} \prod_j N(q_j)^{l_j} = N \left( \prod_i \alpha_i^{k_i} \prod_j q_j^{l_j} \right) = a^2 - ab + b^2$$

for some $a, b \in \mathbb{Z}$.

5. Find (with proof) an ideal $I$ of $\mathbb{Z}[[i]]$ whose quotient $F$ is a field of 9 elements. Is there an ideal whose quotient is a field of 25 elements?

**Solution.** Since 3 is irreducible in $\mathbb{Z}[i]$ ($a^2 + b^2 = 3$ has no integer solution) and $\mathbb{Z}[i]$ is a UFD, $(3) \subset \mathbb{Z}[i]$ is a prime ideal, and thus a maximal ideal by problem 3. Hence, $F = \mathbb{Z}[i]/(3)$ is a field. It is easy to see that the nine elements $\{ a + bi : 0 \leq a, b \leq 2 \}$ of $\mathbb{Z}[i]$ map to distinct elements, and all the elements of $F$. Therefore, $F$ is a field of nine elements. [Alternatively, $\mathbb{Z}[i]/(3) \cong \mathbb{Z}[x]/(3, x^2 + 1) \cong \mathbb{F}_3[x]/(x^2 + 1)$ is a degree 2 field extension over $\mathbb{F}_3$, since $x^2 + 1$ is irreducible over $\mathbb{F}_3$, and hence is a field of $3^2 = 9$ elements.]
(A common mistake was to miscount the number of elements of $\mathbb{Z}[i]/(2)$, by abusing the division algorithm; there are 4, not 9!)

For the second part, here are two solutions.

First solution. Suppose $I$ is an ideal such that $R = \mathbb{Z}[i]/I$ is a field of 25 elements. Then every element of $R$ has order dividing 25, so in particular $25 \in I$. As $I$ is prime, $5 \in I$. However, $\mathbb{Z}/(5)$ has 25 elements (by the same method as above), so $I = (5)$. But then (5) isn’t prime: $5 = (2 + i)(2 - i)$.

Second solution, using what we know now. Suppose we have a ring homomorphism $\varphi : \mathbb{Z}[i] \to \mathbb{F}_{25}$, where $\mathbb{F}_{25}$ is the field of 25 elements. If $\varphi \neq 0$, $\varphi(1) = 1$ (since $\varphi(1)^2 = \varphi(1)$), and thus

$$0 = \varphi(i^2 + 1) = \varphi(i)^2 + 1 = (\varphi(i) - 2)(\varphi(i) - 3).$$

The last equality holds since char = 5. Hence, $\varphi(i) = 2$ or 3, and for any $a, b \in \mathbb{Z}$, $\varphi(a + bi) = a + b\varphi(i) \in \{0, 1, 2, 3, 4\} = \mathbb{F}_5 \subset \mathbb{F}_{25}$. Therefore, there doesn’t exist any surjective homomorphism mapping $\mathbb{Z}[i]$ onto a field of 25 elements. In other words, there doesn’t exist any ideal $I \subset \mathbb{Z}[i]$ such that $\mathbb{Z}[i]/I \cong \mathbb{F}_{25}$.

By a slight extension of these arguments, you can show that if there is an ideal whose quotient is a field of $q$ elements, then $q$ is prime not 3 modulo 4, or the square of a prime that is 3 modulo 4.

6. How many abelian groups are there of order 288?

Solution. 288 = $32 \times 9$. In the direct sum decomposition into primary factors of an abelian group of order 288, the orders of the 2-primary ones can be:

$$\{2, 2, 2, 2\}, \{2, 2, 2, 4\}, \{2, 2, 8\}, \{2, 4, 4\}, \{2, 16\}, \{4, 8\}, \{32\}.$$

Those of the 3-primary ones can be:

$$\{3, 3\}, \{9\}.$$

Hence there are $7 \times 2 = 14$ nonisomorphic abelian groups of order 288.

(Here is is most useful to use the version of the Fundamental Theorem of Abelian groups that separates the group into $p$-parts.)