GRV II, sample questions + answers.

1. (10 points). Let R be a commutative ring with identity. Show that there is a field K for which there exists an onto homomorphism from R to K. (3 points bonus: is this provable without the axiom of choice?)

   Answer: Let M be a maximal ideal, and $K = R/M$. We need the axiom of choice to show that there is a maximal ideal.

2. Let $R = \mathbb{R}[x]/(f(x))$ where $f(x)$ is a non-constant polynomial in $\mathbb{R}[x]$.

   (a) (15 points). Prove that every ideal in R is principal (note: do not write that R is a PID, because if $f(x)$ is reducible then R fails the letter D, domain, in PID).

   Answer: Ideals in R correspond to ideals in $\mathbb{R}[x]$ (a PID!) that contain $f(x)$.

   (b) (5 points). Let $f(x) = x^3 + x$. For this case, list explicitly all ideals of R (no proof is necessary for this question, but your proof for question (a) can be very helpful here. Note: list *all* ideals, including the trivial ones).

   Answer: We have to list all ideals in $\mathbb{R}[x]$ that contain $f(x)$. Since all ideals are principal, each such ideal can be written as $(g(x))$ for some monic factor $g(x)$ of $f(x)$. Since $f(x) = x(x^2+1)$ has 2 irreducible factors, there are $2^2 = 4$ such $g(x)$. Ideals: $(1), (x), (x^2+1), (f(x))$. (Note that (1) is just R, and $(f(x))$ is the zero ideal in R.)

   (c) (10 points). Again $f(x) = x^3 + x$. Give an isomorphism from R to the product $F_1 \times F_2$ for some fields F_1, F_2.

   Answer: By the Chinese Remainder theorem,
   $R = \mathbb{R}[x]/(x(x^2+1)) \cong \mathbb{R}[x]/(x) \times \mathbb{R}[x]/(x^2+1) \cong \mathbb{R} \times \mathbb{C}$.

   (d) (5 points). Again $f(x) = x^3 + x$. The equation $e^2 = e$, how many solutions does this equation have in R?

   Answer: $R \cong \mathbb{R} \times \mathbb{C}$. The equation has two solutions in each component, so there are $2^2 = 4$ solutions all combined (if you want to make this explicit, the idempotents in $\mathbb{R} \times \mathbb{C}$ are (0,0), (0,1), (1,0), and (1,1)).

3. Let $R = \mathbb{Z}[\sqrt{-7}]$.

   (a) (5 points). Show that $1 + \sqrt{-7}$ and 2 are irreducible in R.
   Hint: Introduce the Norm $N(x) := x \cdot \overline{x}$ where $\overline{x}$ is the conjugate of x. Note that $N(xy) = N(x)N(y)$ and if $x = a + b\sqrt{-7}$ then $N(x) = a^2 + 7b^2$. Show that the only units in R are ± 1, there are no elements of Norm 2, and the only elements of Norm 4 are ± 2.

Answer: If $xy = 1$ then $N(x)N(y) = N(1) = 1$ so then $N(x)$ divides 1, but then $N(x) = 1$ because $N(x) \geq 0$. So every unit has Norm 1.

If $x = a + b\sqrt{-7}$ and if $b \neq 0$ then the Norm is at least 7. If $b = 0$ then the Norm is a^2. So there are no elements of Norm 2. If the Norm is 1 then $x = \pm 1$ (a unit). If the Norm is 4 then $x = \pm 2$.

Now let $x = 1 + \sqrt{-7}$. This is irreducible because if $y|x$ then $N(y)|N(x) = 8$ but if y is not an associate of x then $N(y)$ must be $1, 2, 4$ (if $N(y) = 8$ then $N(x/y) = 1$ but then x/y is a unit). There are no elements of Norm 2. And if the Norm is 4 then $y = \pm 2$ but that does not divide x. That means $N(y) = 1$ but then y is a unit. So the only factors of x are associates and units. The proof that 2 is irreducible is similar (using the fact that its Norm is 4 but there are no elements of Norm 2).

(b) (5 points). Show explicitly that R is not a UFD by factoring 8 in two non-equivalent ways as a product of irreducible elements.
Explain why the Norm N is not a Euclidean Norm.

Answer: Let $x = 1 + \sqrt{-7}$. Then $8 = x\overline{x}$ and these two factors are irreducible, so 8 is a product of 2 irreducible factors. But it is also a product of 3 irreducible factors $8 = 2 \cdot 2 \cdot 2$. In a UFD, it is not possible to have two irreducible factors in one factorization, and three in another factorization (moreover, the factors $x, \overline{x}$ are not associates of the factors $2, 2, 2$).
The Norm N can not be Euclidean, because if it were, then R would have been a UFD, which it is not.

(c) (10 points). Let $I \neq R$ be an ideal, and assume that $a, b \in R$, $ab \in I$ while $a, b \notin I$ (in other words, I is not prime). Let $J = (I, a)$. Show that $I \subsetneq J \subsetneq R$.
Hint: the only non-trivial thing to show is that $J \neq R$, which you can show by first showing that $Jb \subseteq I$ while $Rb \not\subseteq I$.

Answer: because of the hint it suffices to show that $Jb \subseteq I$.
$Jb = (Ib, ab)$ all of which is in I.

(d) (10 points). Prove that the ideal (2) is not maximal in R, and that the ideal $(2, 1 + \sqrt{-7})$ is not equal to R.

Answer: This is the same as the previous exercise where $I = (2)$ and $a = 1 + \sqrt{-7}$ and $b = \overline{a}$.

(e) (10 points). Prove that the ideal $(2, 1 + \sqrt{-7})$ is not principal (hint: you may use parts (a)+(d) even if you did not prove them).

Answer: If this ideal was principal, say equal to (x), then since $2 \in (x)$ we have $x|2$. But 2 is irreducible, so (x) is either $(1) = R$ or $(x) = (2)$, but both cases are excluded by part (d).

4. (15 points). Let R be a UFD, and let $f = a_n x^n + \cdots + a_0 x^0 \in R[x]$ with $a_0, a_n \neq 0$. Let K be the field of fractions, and suppose that $x^2 + bx + c \in K[x]$ is a factor of f in $K[x]$. Prove that $a_n \cdot (x^2 + bx + c) \in R[x]$.

   Answer: Let $g = x^2 + bx + c$ then we can write $f = g \cdot h$ with $f \in R[x]$ and $g, h \in K[x]$. With Gauss' lemma we showed that there must then be a non-zero constant $s \in K$ such that sg and $s^{-1}h$ are both in $R[x]$, thus obtaining a factorization of f in $R[x]$ as $(sg)\cdot(s^{-1}h)$. Since $sg = sx^2 + sbx + sc \in R[x]$, it follows that $s \in R$. Since sg is a factor of f, it follows that the leading coefficient of sg is a factor of the leading coefficient of f. So $s|a_n$. So if $sg \in R[x]$, then $a_n g$ must be in $R[x]$ as well.

5. Let G be a subgroup of S_{10} of order $81 = 3^4$. Let $S = \{1, 2, \ldots, 10\}$. The group S_{10} acts on S, and hence, G acts on S as well. Prove that the action of G on S must have a fix point, i.e., prove that there exist an $a \in S$ such that $ga = a$ for all $g \in G$.

   Answer: the length of an orbit under G must divide $|G| = 3^4$. So every orbit must have length $1, 3, 9, 27, \ldots$. All orbits combined must be the set S, which has 10 elements. But 10 is not a sum of $3, 9, 27, \ldots$ so there must be at least one orbit of length 1. Now take a in such an orbit.

6. Let G_1 and G_2 be subgroups of S_{10} of order 81. Prove that G_1 is isomorphic to G_2.

   Answer: G_1, G_2 are 3-Sylow subgroups of S_{10}. They must thus be conjugated by Sylow's theorem. But conjugation is an isomorphism.

7. D_{50}, the dihedral group of order 50, how many elements does it have of order:
   1: 1
   2: 25
   5: 4
   10: 0
   25: 20
   50: 0

   To see this, observe that $D_{2n} = C_n \cup \{n \text{ reflections}\}$. Next, you need to know that if $d|n$ then C_n has $\phi(d)$ elements of order d.

8. (a) List every abelian group of order 600 (up to isomorphism) (in other words, if $G_1 \cong G_2$ then do not list both).

   Answer: $600 = 2^3 3^1 5^2$.
   $3 = 3 = 2 + 1 = 1 + 1 + 1$ (three partitions)
   $1 = 1$ (one partitions)
   $2 = 2 = 1 + 1$ (two partitions).
   So your answer should list $3 \cdot 1 \cdot 2 = 6$ groups: $G \times C_3 \times H$ where $G \in \{C_8, C_4 \times C_2, C_2 \times C_2 \times C_2\}$ and $H \in \{C_{25}, C_5 \times C_5\}$.

(b) List every abelian group of order 64 (up to isomorphism).

I'll only list the partitions, for each partition $n = n_1 + n_2 + \cdots$ the corresponding group is $C_{2^{n_1}} \times C_{2^{n_2}} \times \cdots$. Partitions of 6:
6, 5+1, 4+2, 4+1+1, 3+3, 3+2+1, 3+1+1+1, 2+2+2, 2+2+1+1, 2+1+1+1+1, 1+1+1+1+1+1.

(c) List every abelian group of order 64 that has elements of order 8 but no elements of order 16.

Partitions: 3+3, 3+2+1, and 3+1+1+1.

(d) List every abelian group of order 64 in which the equation $g^2 = e$ has precisely 8 solutions.

Partitions: 4+1+1, 3+2+1, 2+2+2.
To see this, note that $g^2 = e$ has 2 solutions in each $C_{2^{n_i}}$. So for a partition with k terms $n = n_1 + \cdots + n_k$ we get 2^k solutions. For 8 solutions we need $k = 3$.

9. Let $G = \{ax + b \,|\, a \in \mathbb{R}^*,\ b \in \mathbb{R}\}$.
So $G = \{$non-constant linear functions $\mathbb{R} \to \mathbb{R}\}$, which is a group under composition.
Notice that in the first definition of G, you have a in a multiplicative group $\mathbb{R}^*$ and b in an additive group $\mathbb{R}$. Can you write G as a semi-direct product of those two groups?
(if yes, just write down such a semi-direct product (don't forget to include a map from ... to ...). You don't have to prove that your answer is isomorphic to G)

Answer: $\mathbb{R} \rtimes \mathbb{R}^*$. For this to be completely defined we need to give a homomorphism from $\mathbb{R}^*$ to $\mathrm{Aut}(\mathbb{R})$. This homomorphism sends $a \in \mathbb{R}^*$ to $\phi_a \in \mathrm{Aut}(\mathbb{R})$ where ϕ_a sends b to ab.
(if ϕ_a does not look like an automorphism to you, then remember that we do not require ϕ_a to be a ring-automorphism! It only needs to be an automorphism of the additive group $\mathbb{R}$.)

10. Suppose that $d > 1$ and $d|\phi(n)$ where ϕ is the Euler ϕ function
($\phi(n)$ is the number of units in the ring $\mathbb{Z}/(n)$).
Show that there exists a nonabelian group of order nd.

Let p be a prime dividing d. Since p divides the order of the group of units in our ring, there must be a unit $u \in \mathbb{Z}/(n)$ whose order is precisely p, i.e. $u \neq 1$ and $u^p = 1$. Let $\phi_u : \mathbb{Z}/(n) \to \mathbb{Z}/(n)$ denote map $\phi_u(a) = u \cdot a$. Then ϕ_u is an automorphism of the additive group $\mathbb{Z}/(n)$. Now let $C_p =< g >$ be a cyclic group of order p and take the homomorphism from C_p to $\mathrm{Aut}(\mathbb{Z}/(n))$ that sends g to ϕ_u. Now we have constructed a non-abelian group $\mathbb{Z}/(n) \rtimes C_p$. The order is np. If $p < d$ then take a product of this group and $C_{d/p}$. Then we get a non-abelian group of order nd.